MCAFEE

PGP Personal Security für Windows 95, Windows 98, Windows ME, Windows NT und Windows 2000

Benutzerhandbuch

Version 7.0

Copyright © 1990–2000 Network Associates, Inc. und Tochtergesellschaften. Alle Rechte vorbehalten.

PGP*, Version 7.0.0

02-2001. Gedruckt in der EG.

PGP, Pretty Good und Pretty Good Privacy sind eingetragene Warenzeichen von Network Associates, Inc. und/oder den Tochtergesellschaften in den USA und anderen Ländern. Alle weiteren in diesem Dokument enthaltenen eingetragenen und nicht eingetragenen Warenzeichen sind Eigentum der jeweiligen Besitzer.

Einige Teile dieser Software verwenden Verschlüsselungsalgorithmen für öffentliche Schlüssel, die in den US-amerikanischen Patentnummern 4,200,770, 4,218,582, 4,405,829, und 4,424,414 beschrieben werden und ausschließlich durch Public Key Partners lizenziert sind. Die kryptographische Verschlüsselung IDEA™, beschrieben in der US-amerikanischen Patentnummer 5,214,703, ist von Ascom Tech AG lizenziert, und CAST Encryption Algorithm von Northern Telecom Ltd. ist von Northern Telecom, Ltd. lizenziert. IDEA ist ein Warenzeichen von Ascom Tech AG. Network Associates Inc. verfügt möglicherweise über Patente und/oder Patentanmeldungen zum Gegenstand dieser Software oder der Begleitdokumentation. Der Erwerb dieser Software oder Dokumentation berechtigt Sie zu keiner Lizenz für diese Patente. Die Komprimierungscode in PGP wurde von Mark Adler und Jean-Loup Gailly entwickelt und wird mit Genehmigung von der kostenlosen Info-ZIP-Implementierung verwendet. Die LDAP-Software wurde mit Genehmigung der University of Michigan in Ann Arbor zur Verfügung gestellt. Copyright © 1992–1996 Regents of the University of Michigan. Alle Rechte vorbehalten. Dieses Produkt enthält Software, die von der Apache Group zur Verwendung im Apache HTTP-Serverprojekt entwickelt wurde (http://www.apache.org/). Unterstützung für Aktive Hilfe mit Genehmigung von James W. Walker. Copyright © 1995–1999 The Apache Group. Alle Rechte vorbehalten. Weitere Informationen finden Sie in den Textdateien der Software oder auf der PGP-Website. Diese Software basiert zum Teil auf der Arbeit der Independent JPEG Group. Die Schriftart TEMPEST wird mit Genehmigung von Ross Anderson und Marcus Kuhn verwendet. Liste biometrischer Wörter für die Fingerabdruckverifizierung mit Genehmigung von Patrick Juola.

Die zu dieser Dokumentation gehörende Software ist für Sie nur zur individuellen Nutzung lizenziert. Es gelten die Bedingungen der Endbenutzer-Lizenzvereinbarung und der Beschränkten Garantie dieser Software. Die in diesem Dokument enthaltenen Informationen können jederzeit ohne vorherige Ankündigung geändert werden. Network Associates Inc. gewährt keine Garantie dafür, daß diese Informationen Ihren Anforderungen entsprechen oder fehlerfrei sind. Sie können technische Ungenauigkeiten oder Druckfehler enthalten. An diesen Informationen können Änderungen vorgenommen und in neue Auflagen dieser Dokumentation aufgenommen werden, sofern und sobald diese Änderungen von Network Associates International Inc. verfügbar sind.

Der Export dieser Software und Dokumentation kann den in bestimmten Abständen durch das Bureau of Export Administration, United States Department of Commerce (Amt für Exportgenehmigungsanträge des Wirtschaftsministeriums der USA) veröffentlichten Vorschriften und Bestimmungen, die die Ausfuhr und die Wiederausfuhr bestimmter Produkte und technischer Daten beschränken, unterliegen.

McAfee Software Division
PO Box 898
7301 BC Apeldoorn
The Netherlands

Phone: 0800 - 1005262 Germany
Fax: +31 (0) 55 543 4646
E-mail: single_user_europe@NAI.com
http://www.nai.com

® wird gelegentlich anstelle von **®** zum Schutz von Warenzeichen verwendet, die außerhalb der USA eingetragen sind.

BESCHRÄNKTE GARANTIE

Beschränkte Garantie. Network Associates Inc. garantiert für einen Zeitraum von sechzig (60) Tagen ab Kaufdatum, daß die Software im wesentlichen wie in der schriftlichen Begleitdokumentation beschrieben funktioniert. In dem vom gültigen Recht zugelassenen Maße sind die implizierten Gewährleistungen für die Software, soweit diese existieren, auf die Dauer von sechzig (60) Tagen beschränkt. Einige Rechtsordnungen lassen Beschränkungen der Dauer der gesetzlichen Garantie nicht zu, so daß die obige Beschränkung möglicherweise auf Sie nicht anwendbar ist.

Ansprüche des Kunden. Die gesamte Haftung von Network Associates Inc. sowie von deren Anbietern und Ihr alleiniger Anspruch bestehen nach Wahl von Network Associates Inc. entweder (a) in der Rückerstattung des für die Lizenz bezahlten Preises, falls zutreffend, oder (b) in der Reparatur oder dem Ersatz der Software, die der beschränkten Garantie von Network Associates Inc. nicht genügt und die zusammen mit einer Kopie Ihres Kaufbelegs auf Ihre Kosten an Network Associates Inc. zurückgegeben wird. Diese beschränkte Garantie gilt nicht, wenn der Ausfall der Software auf einen Unfall, auf Mißbrauch oder auf fehlerhafte Anwendung zurückzuführen ist. Für eine Ersatz-Software übernimmt Network Associates nur für den Rest der ursprünglichen Garantiefrist oder für dreißig (30) Tage eine Garantie, wobei der längere Zeitraum maßgebend ist. Außerhalb der USA stehen ohne den Nachweis des Erwerbs von einer autorisierten internationalen Quelle weder diese Ansprüche noch andere Produkt-Support-Dienstleistungen von Network Associates Inc. zur Verfügung und sind unter Umständen nicht von Network Associates Inc. verfügbar, sofern sie den Beschränkungen entsprechend den Exportkontrollgesetzen und -bestimmungen der USA unterliegen.

KEINE WEITERE GEWÄHRLEISTUNG. SOWEIT ES DAS GELTENDE RECHT ZULÄSST, ES SEI DENN, ES IST IN DEN ANGABEN ZUR BESCHRÄNKTEN GARANTIE IN DIESEM DOKUMENT ANDERS VORGESEHEN, WERDEN SOFTWARE UND DOKUMENTATION “OHNE MÄNGELGEWÄHR” GELIEFERT. NETWORK ASSOCIATES INC. UND DEREN LIEFERANTEN SCHLIESSEN JEDE WEITERE GEWÄHRLEISTUNG UND ALLE ANSPRÜCHE, OB AUSDRÜCKLICH ODER STILLSCHWEIGEND, EINSCHLIESSLICH DER STILLSCHWEIGENDEN GEWÄHRLEISTUNGEN DER HANDELBARKEIT UND DER EIGNUNG FÜR EINEN BESONDEREN ZWECK, DER ÜBEREINSTIMMUNG MIT DER BESCHREIBUNG, DES ANSPRUCHS UND DER NICHT-VERLETZUNG DER RECHTE DRITTER SOWIE DER BEREITSTELLUNG ODER DER NICHT-BEREITSTELLUNG VON SUPPORT-DIENSTLEISTUNGEN, JEDOCH NICHT AUF DIESE BESCHRÄNKT, AUS. DIESE BESCHRÄNKTE GARANTIE GEWÄHRT IHNEN SPEZIFISCHE RECHTE. ES KÖNNEN IHNEN ANDERE ZUSTEHEN, DIE SICH VON RECHTSORDNUNG ZU RECHTSORDNUNG UNTERSCHEIDEN.

BESCHRÄNKTE HAFTUNG. SOWEIT ES DAS GÜLTIGE RECHT ZULÄSST, SIND WEDER NETWORK ASSOCIATES INC. NOCH DIE LIEFERANTEN FÜR IRGENDWELCHE SCHÄDEN, OB INDIREKTE, ZUFÄLLIGE, FOLGESCHÄDEN, KONKRETE ODER EXEMPLARISCHE SCHÄDEN ODER ENTGANGENEN GEWINN (EINGESCHLOSSEN SCHÄDEN AUS ENTGANGENEM GEWINN, BETRIEBSUNTERBRECHUNG, VERLUST VON GESCHÄFTLICHEN INFORMATIONEN ODER DATEN ODER ANDERE FINANZIELLE EINBUSSEN, JEDOCH NICHT AUF DIESE BESCHRÄNKT), DIE AUFGRUND DER BENUTZUNG DIESES SOFTWAREPRODUKTES ODER DER UNMÖGLICHKEIT DER BENUTZUNG ODER DES VERSÄUMNISSES VON SUPPORT-DIENSTLEISTUNGEN ENTSTEHEN, ERSATZPFLICHTIG, SELBST WENN NETWORK ASSOCIATES VON DER MÖGLICHKEIT EINES SOLCHEN SCHADENS UNTERRICHTET WORDEN IST. IN JEDEM FALL IST DIE KUMULIERTE UND GESAMTE HAFTUNG VON NETWORK ASSOCIATES INC. IHNEN ODER JEGLICHEN DRITTEN GEGENÜBER FÜR SÄMTLICHE VERLUSTE ODER SCHÄDEN AUFGRUND VON RECHTSANSPRÜCHEN, FORDERUNGEN ODER HANDLUNGEN, DIE SICH AUS DIESER LIZENZVEREINBARUNG ERGEBEN ODER DAZU IN BEZUG STEHEN, AUF DEN BETRAG BESCHRÄNKT, DEN SIE FÜR DIE LIZENZ BEZAHLT HABEN. DA EINIGE RECHTSORDNUNGEN DEN HAFTUNGSAUSSCHLUSS ODER DIE HAFTUNGSBESCHRÄNKUNG NICHT ZULASSEN, KANN DIE OBIGE BESCHRÄNKUNG FÜR SIE NICHT GELTEN.

Inhaltsverzeichnis

Teil I: Übersicht

Vorwort 17

Warum sollten Sie sich dieses Handbuch durchlesen? 17

Aufbau dieses Handbuchs 18

So können Sie mit PGP Security und Network Associates in Kontakt treten 20

Kundendienst 20

Technischer Kundendienst 21

Kommentare und Anregungen 22

Empfohlene Literatur 22

Geschichte der Kryptographie 22

Technische Aspekte der Kryptographie 23

Strategisch-politische Aspekte der Kryptographie 24

Netzwerksicherheit 25

Kapitel 1. Grundlagen von PGP 27

PGP als Teil Ihrer Sicherheitsstruktur 27

PGP-Funktionen 29

Grundlagen für die Verwendung von PGP 30

Kapitel 2. Kurze Einführung in PGP 33

Startmenü 33

PGPtools 34

PGP-Plugins für E-Mail-Programme 34

PGP über den Windows-Explorers verwenden 35

PGPtray 36

PGPtray-Optionen “Zwischenablage” und “Aktuelles Fenster” 36

Arbeit produktiver gestalten 37

Hilfe aufrufen 38

Teil II: Mit Schlüsseln arbeiten

Kapitel 3. Schlüssel erstellen und austauschen 41

Begriffe und Konzepte im Zusammenhang mit Schlüsseln 41
Schlüsselpaare erstellen 42
Einprägsame Paßphrasen erstellen 49
Eigenes Schlüsselpaar ändern 50
Sicherungskopien Ihrer Schlüssel erstellen 51
Eigene Schlüssel schützen 51
Was passiert, wenn ich meine Paßphrase vergesse oder meinen Schlüssel verliere? 52
Was versteht man unter “PGP-Schlüsselrekonstruktion”? 52
Öffentliche Schlüssel mit anderen Personen austauschen 55
Eigenen öffentlichen Schlüssel weitergeben 55
Eigenen öffentlichen Schlüssel auf einem Schlüsselserver ablegen 55
Eigenen öffentlichen Schlüssel in eine E-Mail-Nachricht einfügen 57
Eigenen öffentlichen Schlüssel in eine Datei exportieren 57
Öffentliche Schlüssel von anderen Benutzern erhalten 58
Öffentliche Schlüssel von einem Schlüsselserver holen 59
Öffentliche Schlüssel aus E-Mail-Nachrichten entnehmen 61
Schlüssel und X.509-Zertifikate importieren 61
Echtheit eines Schlüssels verifizieren 62
Warum sollte man die Echtheit eines Schlüssels verifizieren? . . 63
Mit digitalen Fingerabdrücken verifizieren 63
Öffentliche Schlüssel überprüfen 64
Mit autorisierten Schlüsselverwaltern arbeiten 64
Was ist ein autorisierter Schlüsselverwalter? 65
Was ist ein höhergestellter Schlüsselverwalter? 65

Kapitel 4. Schlüssel verwalten 67

PGP-Schlüsselbunde verwalten 67
Das PGPkeys-Fenster 68
Definitionen der PGPkeys-Attribute 68

Standardschlüsselpaar am PGP-Schlüsselbund festlegen 73
Schlüssel an Ihrem PGP-Schlüsselbund importieren und exportieren 73
Schlüssel oder Unterschriften aus Ihrem PGP-Schlüsselbund löschen 74
Schlüssel Ihres PGP-Schlüsselbundes deaktivieren und aktivieren 74
Schlüsseleigenschaften überprüfen und festlegen 75
Allgemeine Schlüsseleigenschaften 75
Teilschlüsseleigenschaften 85
Eigenschaften zugeordneter Rücknahmeschlüssel 87
Eigenschaften von zusätzlichen Entschlüsselungsschlüsseln (Additional Decryption Keys, ADK) 90
PGP-Schlüsseln X.509-Zertifikate hinzufügen 91
Schlüssel teilen und wieder zusammensetzen 96
Geteilten Schlüssel erstellen 97
Geteilte Schlüssel zusammensetzen 99
Eigenen Schlüssel auf einem Schlüsselserver aktualisieren 104
Schlüssel rekonstruieren 107

Teil III: Dateien, E-Mail-Nachrichten und Instantnachrichten sichern

Kapitel 5. Sichere Kommunikation per E-Mail 111
Sichere Kommunikation per E-Mail 111
PGP/MIME 111
E-Mail-Nachrichten verschlüsseln und unterschreiben 112
E-Mail-Nachrichten mit den PGP-Plugins verschlüsseln und unterschreiben 112
Nachrichten mit dem Lotus Notes-Plugin verschlüsseln und unterschreiben 117
E-Mails ohne PGP-Plugins verschlüsseln und unterschreiben .120
E-Mail-Nachrichten für Empfängergruppen verschlüsseln 121
Entschlüsseln und Verifizieren von E-Mail-Nachrichten 124
E-Mail-Nachrichten mit den PGP-Plugins entschlüsseln und verifizieren 124

Nachrichten mit dem Lotus Notes-Plugin entschlüsseln und verifizieren 125
Nachrichten ohne PGP-Plugins entschlüsseln und verifizieren 126

Kapitel 6. Dateien sichern 129
Dateien und Ordner mit PGP sichern 129
Dateien verschlüsseln und unterschreiben 129
Dateien entschlüsseln und verifizieren 131
Selbstentschlüsselnde Archive öffnen 132
Dateien mit einem geteilten Schlüssel unterschreiben und entschlüsseln 132
Dateien unwiederbringlich löschen und Speicherplatz bereinigen 132
Dateien mit der PGP-Funktion “Endgültig löschen” löschen 133
Mit dem PGP-Assistenten für das endgültige Löschen von freiem Speicherplatz arbeiten 134
Automatisches Bereinigen von Ordnern und freiem Speicherplatz einrichten 136

Kapitel 7. Instantnachrichten sichern 139
Öffentliche Schlüssel in ICQ austauschen 140
ICQ-Nachrichten verschlüsseln 141

Kapitel 8. Sichere Festplatten mit PGPdisk erstellen 143
PGPdisk-Grundlagen 143
PGPdisk-Funktionen 143
Sinn und Zweck von PGPdisk 144
Kurze Einführung in PGPdisk 145
Auf PGPdisk zugreifen 146
Mit PGPdisk in einem Windows-Explorer-Fenster arbeiten 147
So arbeiten Sie mit PGPdisk in einem PGPdisk-Editor 148
PGPdisk verwenden 150
Neues PGPdisk-Volume erstellen 150
Paßphrase für ein PGPdisk-Volume ändern 154
Alternative Benutzer zu einem PGPdisk-Volume hinzufügen 155
Alternative Benutzer von einem PGPdisk-Volume entfernen 157
PGPdisk-Volume laden 158

Geladenes PGPdisk-Volume verwenden 158
PGPdisk-Volume entladen 159
Eigenschaften für ein PGPdisk-Volume festlegen 160
PGPdisk-Volumes verwalten 162
PGPdisk-Volumes automatisch laden 162
PGPdisk-Dateien auf einem entfernten Server laden 163
Sicherungskopien von PGPdisk-Volumes erstellen 163
PGPdisk-Volumes austauschen 164
Größe eines PGPdisk-Volumes ändern 165
PGPdisk-Volumes neu verschlüsseln 166
Technische Daten und Sicherheitsvorkehrungen 167
Überblick über PGPdisk-Volumes 167
Die PGPdisk-Verschlüsselungsalgorithmen 168
Besondere Sicherheitsvorkehrungen von PGPdisk 169
Löschen der Paßphrase 169
Schutz des virtuellen Speichers 169
Schutz vor statischen Ionenmigrationen im Arbeitsspeicher . . . 169
Andere Sicherheitsvorkehrungen 170

Teil IV: Netzwerkkommunikation mit PGPnet sichern

Kapitel 9. PGPnet-Grundlagen 175
Zu PGPnet 175
Was ist eine persönliche Firewall? 176
Was ist ein Angrifferkennungssystem? 177
Was ist ein VPN? 178
VPN-Begriffe 179

Kapitel 10. Kurze Einführung in PGPnet 183
PGPnet starten 183
PGPnet aktivieren und deaktivieren 183
PGPnet beenden 184
PGPnet-Funktionen 184
Das PGPtray-Symbol 185
Das PGPnet-Fenster auf einen Blick 186
Menüs 186

Registerkarten 187
Statusleiste 188
Status der vorhandenen Sicherheitsverbindungen (SAs) überprüfen 189
SAs einrichten und beenden 192
Hostliste importieren 193
Hostliste exportieren 193
Kommunikation mit anderen Rechnern blockieren 193
Hosts blockieren und die Kommunikationsquelle zurückverfolgen . . 195
Angreifer aufspüren 195
Hosts aus der Liste der blockierten Hosts entfernen 197
PGPnet-Protokolleinträge anzeigen 197
Sichere Netzwerkschnittstelle ändern: "PGPnet – Adapter einstellen" 198

Kapitel 11. Die PGPnet-Firewall- und -Angrifferkennungsfunktion konfigurieren 201
Die persönliche Firewall in PGPnet konfigurieren 202
Vordefinierten Schutzgrad verwenden 203
Benutzerdefinierten Schutzgrad erstellen 209
Das persönliche Angrifferkennungssystem (IDS) in PGPnet konfigurieren 216

Kapitel 12. Die PGPnet-Funktion "VPN" konfigurieren 221
Schritt 1. PGPnet-Programm starten 222
Schritt 2. Authentisierungsschlüssel bzw. -zertifikat auswählen 222
Schritt 3a. Hostliste importieren 223
Schritt 3b. Host, Teilnetz oder Gateway hinzufügen 224
Schritt 4. SA einrichten 224
Assistenten für das Hinzufügen von Hosts verwenden 226
Benötigte Informationen 227
Host hinzufügen 227
Teilnetz oder Gateway hinzufügen 229
Host-, Teilnetz- oder Gateway-Eintrag ändern 233
Host-, Teilnetz- oder Gateway-Eintrag entfernen 233

Expert-Modus: Hosts, Gateways oder Teilnetze ohne Assistenten hinzufügen 234
Expert-Modus aktivieren und deaktivieren 235
DNS-Suche: IP-Adresse eines Hosts suchen 236
Gemeinsames Geheimnis 237
Entfernte Authentisierung 237
Vorlage eines bestimmten Schlüssels oder eines bestimmten Zertifikats vom Host fordern 237
Die Funktionen “Abrufen der virtuellen Identität” und “Exklusiver Gateway” 239

Teil V: Anhänge und Glossar

Anhang A. Optionen festlegen 243

PGP-Optionen festlegen 244
Allgemeine Optionen festlegen 244
Dateioptionen festlegen 248
E-Mail-Optionen festlegen 250
HotKey-Optionen festlegen 253
Serveroptionen festlegen 255
CA-Optionen festlegen 258
Erweiterte Optionen festlegen 259
Optionen für die persönliche Firewall festlegen 263
Optionen für das persönliche IDS festlegen 263
VPN-Optionen festlegen 263
Werte für die automatische Schlüsselerneuerung festlegen . . . 266
Optionen für die VPN-Authentisierung festlegen 267
Optionen auf der Registerkarte “VPN – Erweitert” festlegen 270
Zulässige entfernte Vorschläge hinzufügen und entfernen 276
Mit IKE- und IPsec-Vorschlägen arbeiten 276
PGPdisk-Optionen festlegen 279

Anhang B. Problembehebung in PGP 283

Anhang C. Problembehebung in PGPnet 287

PGPnet-Fehlermeldungen 287

Zusätzliche Tips 289

Grundlagen der Authentisierung 289

Registerkarte “VPN-Authentisierung” 290

Dialogfeld “Host/Gateway”: Entfernte Authentisierung 291

Anhang D. Von der PGPnet-Funktion IDS erkannte häufig vorkommende Angriffe 293

Anhang E. Liste biometrischer Worte 297

Liste biometrischer Worte 297

Anhang F. Produkt-Support 303

Kontakt mit McAfee 303

Customer Service 303

Technischer Support 304

Support über das Web 304

Support-Foren und telefonische Kontaktaufnahme 304

Glossar 305

Index 319

Teil I: Übersicht

- **Vorwort**
- **Kapitel 1: Grundlagen von PGP**
- **Kapitel 2: Kurze Einführung in PGP**

Vorwort

Als Bestandteil der Sicherheitswerkzeuge Ihres Unternehmens schützt PGP eines Ihrer wichtigsten Güter: *Ihre Daten*. Herkömmlicherweise bewahren viele Unternehmen ihre wichtigen Daten in speziell gesicherten und verschlossenen Räumen auf, zu denen nur Mitarbeiter Zutritt haben, die sich entsprechend ausweisen können. PGP ist ein wertvolles Hilfsmittel, das Sie bei der Gewährleistung der Sicherheit und Integrität der Daten und Nachrichten in Ihrem Unternehmen unterstützt. Die Verletzung der Vertraulichkeit von Informationen hat in den meisten Fällen katastrophale Folgen für die betroffenen Unternehmen.

In diesem Handbuch wird beschrieben, wie Sie PGP® Desktop Security für Windows 95, 98, ME, 2000 und Windows NT verwenden können. PGP Desktop Security (in diesem Handbuch auch einfach als PGP bezeichnet) besitzt viele neue Funktionen, über die Sie sich in der im Produkt enthaltenen *ReadMe.txt*-Datei informieren können.

Warum sollten Sie sich dieses Handbuch durchlesen?

PGP Desktop Security wird typischerweise in Unternehmensumgebungen eingesetzt und durch einen Netzwerkadministrator auf einem Rechner im Netzwerk installiert, der als PGP-Verwaltungsrechner bezeichnet wird. Mit Hilfe von PGPadmin, einer Komponente des Softwarepakets, auf die normale Benutzer nicht zugreifen können, legt der Netzwerkadministrator die für alle Benutzer gültigen Einstellungen fest und erstellt ein Installationsprogramm. Das Installationsprogramm wird an die einzelnen Benutzer auf dem Netzwerk weitergegeben, die dann mit Hilfe dieses Programms PGP auf ihren Rechnern installieren.

Wenn Sie dieses Handbuch lesen, handelt es sich bei Ihnen aller Wahrscheinlichkeit nach um einen Benutzer eines Hosts eines Unternehmensnetzwerkes, das mit PGP Desktop Security arbeitet. In diesem Benutzerhandbuch werden die Funktionen von PGP beschrieben, und es wird erläutert, wie Sie PGP auf Ihrem Rechner konfigurieren und so auf Ihre individuellen Sicherheitsanforderungen zuschneiden können.

HINWEIS: Wenn Sie sich noch nicht näher mit Kryptographie beschäftigt haben und sich einen Überblick über Terminologie und Grundlagen der Anwendung von PGP verschaffen möchten, finden Sie weitere Informationen in dem dem Produkt beiliegenden Handbuch *Einführung in die Kryptographie*.

Aufbau dieses Handbuchs

Das Handbuch ist in folgende Teile und Kapitel unterteilt:

Teil I, “Grundlagen”

In diesem Teil werden die PGP-Funktionen vorgestellt, und Sie erhalten einen kurzen Überblick über die PGP-Benutzeroberfläche. Teil I enthält die folgenden Kapitel:

- Kapitel 1, “Grundlagen von PGP”, bietet einen Überblick über den Leistungsumfang des Programms und erläutert den Platz, den PGP in der übergreifenden Sicherheitsstruktur eines Unternehmens hat.
- Kapitel 2, “Kurze Einführung in PGP”, bietet eine kurze Einführung dazu, wie Sie von Ihrem Desktop aus auf die PGP-Dienstprogramme zugreifen können.

Teil II, “Mit Schlüsseln arbeiten”

In diesem Teil wird der wichtige Begriff des *Schlüssels* erläutert, der für die Datenverschlüsselung fundamentale Bedeutung hat. Teil II enthält die folgenden Kapitel:

- Kapitel 3, “Schlüssel erstellen und austauschen”, erläutert den Begriff des Datenverschlüsselungsschlüssels und beschreibt, wie Sie Schlüssel erstellen, schützen, austauschen und auf Echtheit überprüfen können.
- Kapitel 4, “Schlüssel verwalten”, enthält detaillierte Informationen zur Schlüsselwartung, also wie Sie Ihren *Schlüsselbund* verwalten, *Schlüsseleigenschaften* überprüfen und ändern und *geteilte Schlüssel* erstellen können.

Teil III, “Dateien und Kommunikation sichern”

In diesem Teil wird erläutert, wie Sie Ihre Datenverschlüsselungsschlüssel zum Sichern von Daten verwenden können, die Sie von Ihrem Computer senden bzw. auf diesem speichern. Teil III enthält die folgenden Kapitel:

- Kapitel 5, “Sichere Kommunikation per E-Mail”, beschreibt, wie Sie verschlüsselte E-Mails senden und wie Sie E-Mails, die Sie erhalten, entschlüsseln und verifizieren können.
- Kapitel 6, “Dateien sichern”, beschreibt, wie Sie mit PGP Dateien sicher verwalten können, die Sie entweder als E-Mail senden oder auf Ihrem Computer speichern möchten.
- Kapitel 7, “Instantnachrichten sichern”, beschreibt, wie Sie mit Hilfe des PGP-Plugins für ICQ (einer Anwendung, mit der Sie über das Internet in Echtzeit kommunizieren können) Ihre Instantnachrichten sichern können.

- Kapitel 8, “Sichere Festplatten mit PGPdisk erstellen”, beschreibt, wie Sie die Funktion “PGPdisk”, mit der ein Teil Ihrer Festplatte als separater “Datenträger” reserviert werden kann, zum Speichern gesicherter Dateien verwenden können.

Teil IV, “Netzwerkkommunikation mit PGPnet sichern”

In diesem Teil werden die Funktionen von PGPnet beschrieben. Dabei handelt es sich um ein PGP-Werkzeug, mit dem Sie Ihre persönliche Firewall und ein persönliches Angrifferkennungssystem (IDS) einrichten und VPNs (Virtual Private Networks) mit vertrauenswürdigen Benutzern erstellen können, die nicht direkt mit Ihrem Netzwerk verbunden sind. Außerdem finden Sie in den in Teil IV enthaltenen Kapiteln Informationen dazu, wie Sie beim Konfigurieren der PGPnet-Funktionen diese der Sicherheit Ihrer Arbeitsstation anpassen können. Teil IV enthält die folgenden Kapitel:

- Kapitel 9, “PGPnet-Grundlagen”, bietet einen Überblick über persönliche Firewalls, Angrifferkennungssysteme (IDS) und VPNs (Virtual Private Networks).
- Kapitel 10, “Kurze Einführung in PGPnet”, führt Sie in die Aspekte der PGP-Benutzeroberfläche im Zusammenhang mit PGPnet ein.
- Kapitel 11, “Die PGPnet-Firewall- und -Angrifferkennungsfunktion konfigurieren”, beschreibt, wie Sie mit Hilfe von PGPnet eine persönliche Firewall und ein persönliches IDS auf Ihrem Computer einrichten können.
- Kapitel 12, “Die PGPnet-Funktion “VPN” konfigurieren”, beschreibt, wie Sie mit PGPnet ein VPN (Virtual Private Network) einrichten und Ihren Anforderungen entsprechend gestalten können.

Teil V, “Anhänge und Glossar”

Dieser Teil enthält Informationen dazu, wie Sie PGP darüber hinaus an die Bedürfnisse Ihres Computers anpassen können und welche Möglichkeiten der Fehlerbehebung Sie haben, wenn Sie bei der Arbeit mit PGP auf Probleme stoßen. Als nützliche Referenz finden Sie in diesem Teil auch ein Glossar mit Definitionen der Begriffe, die im Zusammenhang mit Netzwerksicherheit eine Rolle spielen. Teil V enthält die folgenden Anhänge:

- Anhang A, “Optionen festlegen”, erläutert, wie Sie im Dialogfeld “Optionen” auf Ihrem Computer eine PGP-Version erstellen können, die Ihren Anforderungen am besten entspricht.
- Anhang B, “Problembehebung in PGP”, enthält Hinweise zur Lösung von Problemen, auf die Sie bei der Arbeit mit PGP stoßen.

- Anhang C, “Problembehebung in PGPnet”, enthält Hinweise zur Lösung von Problemen, auf die Sie bei der Arbeit mit der PGP-Funktion “PGPnet” stoßen.
- Anhang D, “Von der PGPnet-Funktion IDS erkannte häufig vorkommende Angriffe”, enthält eine Aufstellung der Angriffe, die vom IDS in PGPnet blockiert wurden, samt einer Beschreibung und einer Risikoeinstufung für jeden einzelnen Angriff.
- Anhang E, “Liste biometrischer Worte”, enthält Listen biometrischer Wörter und erläutert, wie diese von PGP verwendet werden.
- Glossar, Seite 305 enthält Definitionen für viele Begriffe, die im Zusammenhang mit PGP und Netzwerksicherheit verwendet werden.

So können Sie mit PGP Security und Network Associates in Kontakt treten

Kundendienst

Network Associates vermarktet und unterstützt die Produktlinien auch weiterhin von jeder der neuen unabhängigen Geschäftseinheiten aus. Sie können daher Ihre Fragen, Anmerkungen oder Forderungen zur erworbenen Software, Ihre Registrierung u. ä. an den Network Associates-Kundendienst unter folgender Adresse richten:

Network Associates International B.V.
Gatwickstraat 25
NL-1043 GL Amsterdam

Der Kundendienst ist montags bis freitags von 6.00 UHR bis 18.00 UHR zu erreichen.

Firmenkunden können darüber hinaus folgende Kontaktmöglichkeiten nutzen:

Tel.:	+31(20)5866 100
E-Mail:	support_retail_de@nai.com
World Wide Web:	http://www.nai.com

Technischer Kundendienst

PGP Security und Network Associates haben es immer als eine der wichtigsten Aufgaben betrachtet, die Kunden voll zufriedenzustellen. Die Unternehmen setzen diese Tradition fort, indem sie auf ihren Websites Antworten und Lösungen für eine Vielzahl von technischen Problemen bereitstellen. Wenn Sie also Antworten auf häufig gestellte Fragen suchen, aktualisierte Software-Versionen von PGP Security- und Network Associates-Produkten herunterladen oder die neuesten Nachrichten und Informationen zu Viren erhalten möchten, sollten Sie zuerst auf diesen Websites nachsehen..

World Wide Web: http://www.nai.com

Damit das Network Associates-Kundendienstpersonal Ihre Fragen schnell und effizient beantworten kann, benötigen wir Informationen über Ihren Computer und die von Ihnen verwendete Software. Bitte geben Sie bei einer Kontaktaufnahme mit uns immer auch die folgenden Informationen an:

- Programmname und Versionsnummer
- Computermarke und -modell
- weitere an Ihren Computer angeschlossene Hardware oder Peripheriegeräte
- Art des Betriebssystems und Versionsnummern
- Netzwerkname, Betriebssystem und Version
- installierte Netzwerkkarte (sofern zutreffend)
- Hersteller, Modell und Baudrate des Modems (sofern zutreffend)
- relevante Browser und Anwendungen sowie deren Versionsnummern (sofern zutreffend)
- Wie läßt sich Ihr Problem reproduzieren: wann ist es aufgetreten, läßt es sich regelmäßig reproduzieren und wenn ja unter welchen Umständen?
- Informationen, wie wir Sie per Telefon, Fax oder E-Mail erreichen können

Kommentare und Anregungen

PGP Security ist sehr an Ihren Anmerkungen interessiert und behält sich das Recht vor, die von Ihnen zur Verfügung gestellten Informationen auf geeignete Weise zu verwenden, ohne daß sich daraus Verpflichtungen irgendeiner Art ergeben. Anmerkungen zur Dokumentation senden Sie bitte an **tns_documentation@nai.com**.

Empfohlene Literatur

In diesem Abschnitt finden Sie Empfehlungen zu Websites, Büchern und regelmäßigen Veröffentlichungen zur Geschichte der Kryptographie, ihren technischen Aspekten und strategisch-politischen Fragen im Zusammenhang mit diesem Thema. Außerdem erhalten Sie hier einen Überblick über die Websites, von denen Sie PGP gefahrlos herunterladen können.

Geschichte der Kryptographie

- *The Code Book: The Evolution of Secrecy from Mary, Queen of Scots, to Quantum Cryptography*, Simon Singh, Doubleday & Company, Inc., 1999, ISBN 0-385-49531-5.
- *The Codebreakers: The Story of Secret Writing*, David Kahn, Simon & Schuster Trade, 1996, ISBN 0-684-83130-9 (Aktualisierung der Ausgabe von 1967). In diesem Buch wird die Geschichte der Codierung und der Entschlüsselung von Codes von den alten Ägyptern bis zum Ende des 2. Weltkriegs beschrieben. Dies ist eine überarbeitete Fassung der bereits in den 60er Jahren erschienenen Erstfassung. Das Buch enthält zwar keine Darstellung der kryptographischen Verfahrensweisen, diente aber der gesamten heutigen Generation von Kryptographen als Anregung und Inspirationsquell.

Technische Aspekte der Kryptographie

Websites

- www.iacr.org: International Association for Cryptologic Research (IACR). Die IACR veranstaltet Kryptographiekonferenzen und veröffentlicht Zeitschriften.
- www.pgpi.org: Internationale PGP-Website, die nicht von PGP Security, Inc. bzw. Network Associates, Inc. unterhalten wird. Inoffizielle aber umfangreiche Quelle für PGP.
- www.nist.gov/aes: Website des Projekts "Advanced Encryption Standard (AES)" des National Institute of Standards and Technology (NIST) – das vielleicht interessanteste laufende Projekt zum Thema Kryptographie.
- www.ietf.org/rfc/rfc2440.txt: Spezifikation für den IETF-Standard OpenPGP.

Bücher und regelmäßige Veröffentlichungen

- *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, 2. Auflage, Bruce Schneier, John Wiley & Sons, 1996; ISBN 0-471-12845-7. Wenn Sie als Einstieg in die Kryptographie nur ein Buch kaufen können, sollten Sie sich für dieses entscheiden.
- *Handbook of Applied Cryptography*, Alfred Menezes, Paul van Oorschot und Scott Vanstone, CRC Press, 1996; ISBN 0-8493-8523-7. Dieses Buch sollten Sie nach dem Buch von Schneier als nächstes erwerben. Es enthält viele komplizierte mathematische Zusammenhänge, eignet sich aber dennoch auch für Benutzer, die mit den mathematischen Zusammenhängen nicht so viel anfangen können.
- *Journal of Cryptology*, International Association for Cryptologic Research (IACR). Siehe dazu www.iacr.org.
- *Advances in Cryptology*, jährlich vom Springer-Verlag veröffentlichte Konferenzbeiträge der IACR-CRYPTO-Konferenzen. Siehe dazu www.iacr.org.
- *Cryptography for the Internet*, Philip Zimmermann, Scientific American, October 1998 (lehrreiche Einführung).
- *The Twofish Encryption Algorithm: A 128-Bit Block Cipher*, Bruce Schneier, et al, John Wiley & Sons, Inc., 1999; ISBN: 0471353817. Enthält detaillierte Informationen zum Twofish-Verschlüsselungsalgorithmus – von den Entwicklungskriterien bis hin zu seiner Kryptoanalyse.

Strategisch-politische Aspekte der Kryptographie

Websites

- www.epic.org: Webseite des Electronic Privacy Information Center (Informationszentrum für den elektronischen Schutz elektronischer Daten).
- www.crypto.org—Internet Privacy Coalition.
- www.eff.org: Webseite der Electronic Frontier Foundation.
- www.privacy.org: Die Datenschutz- und Kryptographie-Seite. Hervorragende Informationsquelle zu Datenschutzfragen.
- www.cdt.org: Webseite des Center for Democracy and Technology (Zentrum für Demokratie und Technik).
- www.pgp.com/phil: Homepage von Phil Zimmermann, seine Aussagen vor dem US-Senat usw.

Bücher

- *Privacy on the Line: The Politics of Wiretapping and Encryption*, Whitfield Diffie und Susan Landau, The MIT Press, 1998, ISBN 0-262-04167-7. In diesem Buch werden die Geschichte der Kryptographie und Kommunikationssicherheit sowie strategisch-politische Fragen erörtert, die damit im Zusammenhang stehen. Ein hervorragendes Buch, das auch für Anfänger und technisch nicht so versierte Leser geeignet ist. Es enthält Informationen, die selbst vielen Experten nicht bekannt sind.
- *Technology and Privacy: The New Landscape*, Philip Agre und Marc Rotenberg, The MIT Press, 1997; ISBN 0-262-01162-x.
- *Building in Big Brother, The Cryptographic Policy Debate*, bearbeitet von Lance Hoffman, Springer-Verlag, 1995; ISBN 0-387-94441-9.
- *The Official PGP User's Guide*, Philip Zimmermann, The MIT Press, 1995; ISBN 0-262-74017-6. PGP im praktischen Einsatz – von Philip Zimmermann selbst geschrieben.
- *The Code Book: The Evolution of Secrecy from Ancient Egypt to Quantum Cryptography*, Simon Singh, Doubleday & Company, Inc., September 2000; ISBN: 0385495323. Dieses Buch eignet sich hervorragend als Einführung für diejenigen, die verstehen wollen, wie sich das menschliche Bedürfnis nach Wahrung der Privatsphäre in der Kryptographie manifestiert hat.

Netzwerksicherheit

Bücher

- *Building Internet Firewalls*, Elizabeth D. Zwicky, D. Brent Chapman, Simon Cooper und Deborah Russell (Editor), O'Reilly & Associates, Inc., 2000; ISBN: 1565928717. Ein praktisches Handbuch zu Fragen der Planung, Entwicklung und Wartung von Firewalls.
- *Firewalls and Internet Security: Repelling the Wily Hacker*, William R. Cheswick, Steven M. Bellovin, Addison Wesley Longman, Inc., 1994; ISBN: 0201633574. Praxistips zum Schutz von Netzwerken vor Hackerangriffen über das Internet.
- *Hacking Exposed: Network Security Secrets and Solutions*, Stuart McClure, Joel Scambray und George Kurtz, The McGraw-Hill Companies, 1999; ISBN: 0072121270. Neuester Stand der Erkenntnisse auf dem Gebiet des Eindringens in Computer und Netzwerke aus Angreifer- und Verteidigersicht.

Grundlagen von PGP 1

In diesem Kapitel erhalten Sie einen Überblick darüber, wie sich PGP Desktop Security in die übergeordnete Sicherheitsstruktur Ihrer Organisation einpaßt und diese stärkt. Funktionen und Merkmale von PGP werden vorgestellt, und Sie finden hier eine kurze Darstellung der Schritte, die Sie normalerweise bei der Arbeit mit PGP ausführen müssen.

PGP als Teil Ihrer Sicherheitsstruktur

Ein Unternehmen hat verschiedene Mittel und Möglichkeiten, Informationen zu schützen. Es kann die Türen zum Gebäude sowie bestimmte Räume im Gebäude physisch schließen und damit den Zutritt zu diesen Orten auf befugtes Personal einschränken. Es kann festlegen, daß alle Angestellten beim Anmelden im Netzwerk ein Paßwort eingeben müssen. Es kann einen Computer als Firewall-Server einrichten, den der gesamte ankommende Datenverkehr passieren muß, um auf diese Weise den Datenverkehr zwischen dem Unternehmensnetzwerk und anderen Netzwerken zu steuern. Dies sind nur einige Beispiele für die Möglichkeiten, mit denen ein Unternehmen seine Informationen vor unbefugtem Zugriff sichern kann.

PGP Desktop Security erweitert dieses Sicherheitssystem noch, indem es die Daten auf *einzelnen* Computern schützt. Eine erhöhte Sicherheit wird dabei erreicht durch:

1. das Verschlüsseln von Daten, einschließlich E-Mail-Nachrichten, gespeicherten Dateien und Instantnachrichten
2. die Verwendung eines VPN (Virtual Private Network) für die sichere Kommunikation über Netzwerkgrenzen hinweg
3. persönliche Firewalls und Angriffserkennungsfunktionen

Durch Datenverschlüsselung sind die Benutzer in der Lage, sowohl Informationen zu schützen, die sie absenden (wie z. B. E-Mails) als auch Informationen, die sie auf ihrem eigenen Computer speichern. Dateien und Nachrichten werden mit einem benutzereigenen *Schlüssel* verschlüsselt, der in Verbindung mit Verschlüsselungsalgorithmen Daten produziert, die nur von den tatsächlich gewünschten Empfängern entschlüsselt werden können.

Die Datenverschlüsselung ist auch ein wichtiger Teil eines VPN (Virtual Private Network): Die Informationen werden zunächst verschlüsselt und dann in dieser sicheren Form über das Internet, einem ansonsten sehr unsicheren Medium, an den entfernten Host gesendet. VPNs sind ein Merkmal von PGPnet, einem PGP-Werkzeug zum Einrichten von VPNs, persönlichen Firewalls und Angriffserkennungssystemen.

Persönliche Firewalls dienen, wie auch die Firewall-Server eines Netzwerks, als Steuerungspunkt für den Datenverkehr. Der Firewall-Server eines Netzwerks überprüft die von außen ankommenden Informationen daraufhin, ob sie in das Netzwerk gelangen dürfen, während eine persönliche Firewall die beim jeweiligen Einzelcomputer eingehenden Informationen überprüft und gegebenenfalls nicht passieren läßt.

Für einen Firewall-Server sind aber alle Informationen, die ihren Ursprung im jeweiligen Netzwerk haben, generell *vertrauenswürdig*. Was aber passiert, wenn eine nicht vertrauenswürdige Person sich Zugang zu einem Host innerhalb des Netzwerks verschafft? Persönliche Firewalls schützen die einzelnen Computer innerhalb des Netzwerks sowohl gegen Angriffe von außen als auch gegen Angriffe *von innen*, also aus dem eigenen Netzwerk.

Ein weiterer Vorteil von persönlichen Firewalls besteht darin, daß die einzelnen Benutzer die Firewall-Filter für ihren Computer ihren persönlichen Wünschen und Anforderungen entsprechend konfigurieren können. Während beispielsweise einige Benutzer ihre Arbeitsstationen nicht für TELNET-Sitzungen konfigurieren möchten, kann einer der Benutzer für seinen Computer TELNET-Sitzungen zulassen.

Das dritte Hauptmerkmal von PGP ist seine Angriffserkennungsfunktion IDS (Intrusion Detection System). Wenn IDS aktiviert ist, sucht es nach verdächtigen Aktivitäten und protokolliert diese, wenn es auf eine solche Aktivität stößt. Sie können das IDS auch so konfigurieren, daß beim Erkennen eines Angriffs ein Signalton ertönt und der Angriff sowie der gesamte zukünftige Verkehr des Angreifers blockiert wird. Die IDS-Funktion von PGP zeichnet sich dadurch aus, daß es sowohl vor Angriffen von außen als auch vor Angriffen aus dem eigenen Unternehmensnetzwerk schützt.

Soweit ein kurzer Überblick über die ganz allgemeine Funktionsweise von PGP. Im nächsten Abschnitt finden Sie eine Aufstellung der PGP-Funktionen und -Merkmale sowie Verweise auf bestimmte Kapitel in diesem Benutzerhandbuch mit weiterführenden Informationen zum jeweiligen Thema.

PGP-Funktionen

PGP enthält verschiedene Funktionen und Dienstprogramme, die Ihnen beim Sichern Ihrer E-Mails, Ihrer Dateien, Ihrer Datenträger und Ihres Netzverkehrs durch Verschlüsseln und Authentisieren helfen.

Mit PGP können Sie folgendes tun:

- **Verschlüsseln/unterschreiben und entschlüsseln/verifizieren, und zwar in allen Anwendungen:** Über die PGP-Menüs und die E-Mail-Plugins können Sie aus jeder Anwendung heraus auf die PGP-Funktionen zugreifen. Informationen, wie Sie auf PGP zugreifen können, finden Sie in Kapitel 2, “Kurze Einführung in PGP”. Hinweise, wie Sie beim Verschlüsseln / Unterschreiben und Entschlüsseln / Verifizieren vorgehen müssen, finden Sie in ”Teil III: Dateien, E-Mail-Nachrichten und Instantnachrichten sichern”.
- **Schlüssel erstellen und verwalten:** Mit Hilfe von PGPkeys können Sie Ihr eigenes PGP-Schlüsselpaar sowie alle öffentlichen Schlüssel anderer Benutzer, die Sie Ihrem öffentlichen Schlüsselbund hinzugefügt haben, erstellen, anzeigen und warten. Informationen dazu, wie Sie ein Schlüsselpaar erstellen können, finden Sie in Kapitel 3, “Schlüssel erstellen und austauschen”. Hinweise zur Verwaltung Ihrer Schlüssel erhalten Sie in Kapitel 4, “Schlüssel verwalten”.
- **Selbstentschlüsselnde Archive (SDAs) erstellen:** Sie können selbstentschlüsselnde, ausführbare Dateien erstellen, die andere Personen bei Eingabe des richtigen Paßworts entschlüsseln können. Diese Funktion ist besonders dann hilfreich, wenn verschlüsselte Dateien an Personen verschickt werden sollen, auf deren Computer PGP nicht installiert ist. Weitere Informationen zu SDAs finden Sie in Kapitel 6, “Dateien sichern”.
- **Sichere Volumes auf Ihrer Festplatte erstellen:** Mit Hilfe von PGPdisk können Sie einen Teil Ihrer Festplatte für die sichere Speicherung von Daten verschlüsseln. Weitere Informationen zu PGPdisk finden Sie in Kapitel 8, “Sichere Festplatten mit PGPdisk erstellen”.
- **Dateien und Ordner unwiederbringlich löschen und freien Speicherplatz bereinigen:** Mit Hilfe des Dienstprogramms “PGP Wiper” können Sie Ihre vertraulichen Dateien und Ordner so löschen, daß keine Datenfragmente auf der Festplatte verbleiben. Das Dienstprogramm “PGP Free Space Wiper” kann zum endgültigen Löschen von Datenfragmenten aus bereits gelöschten Dateien und Programmen verwendet werden, die weiterhin Speicherplatz belegen. Beide Dienstprogramme sorgen dafür, daß Ihre gelöschten Daten nicht wiederherstellbar sind. Informationen dazu, wie Sie Dateien und Ordner endgültig löschen und freien Speicherplatz bereinigen können, finden Sie im Abschnitt “Dateien unwiederbringlich löschen und Speicherplatz bereinigen” auf Seite 132.

- **Netzwerkverkehr sicher gestalten.** Mit PGPnet, einem *Virtual Private Network (VPN)*, können Sie sicher und kostengünstig mit anderen PGPnet-Benutzern über das Internet kommunizieren. PGPnet enthält darüber hinaus eine persönliche Firewall für PGPnet-Benutzer sowie eine Angriffserkennungsfunktion, die Angreifer erkennt und blockiert, die versuchen, auf Ihr System zuzugreifen und es von außen zu steuern oder zum Absturz zu bringen. Weitere Informationen zu PGPnet und dessen Komponenten finden Sie in ”Teil IV: Netzwerkkommunikation mit PGPnet sichern”.

Grundlagen für die Verwendung von PGP

1. **Installieren Sie PGP auf Ihrem Computer.**

   Ausführliche Anweisungen zum Installieren finden Sie im *PGP-Installationshandbuch* bzw. in der Datei *ReadMe.txt* im Installationsordner des Produkts.

   HINWEIS: Wenn Sie Benutzer innerhalb eines Unternehmens sind, sollten Sie sich bei Ihrem Administrator erkundigen, ob Sie spezielle Installationsanweisungen befolgen müssen.

   ---

2. **Erstellen Sie ein aus einem privaten und einem öffentlichen Schlüssel bestehendes Schlüsselpaar.**

   Bevor Sie PGP einsetzen können, müssen Sie ein Schlüsselpaar erstellen.

   Sie können dabei wählen, ob Sie bereits während des PGP-Installationsvorgangs ein neues Schlüsselpaar erstellen oder ob Sie dies später in PGPkeys tun möchten.

   Ein Schlüsselpaar benötigen Sie, um:

   - Informationen zu verschlüsseln
   - Informationen, die mit Ihrem Schlüssel verschlüsselt wurden, wieder zu entschlüsseln
   - Informationen zu unterschreiben

   Weitere Informationen zum Erstellen eines Schlüsselpaares finden Sie im Abschnitt “Schlüsselpaare erstellen” auf Seite 42.

3. **Tauschen Sie Ihre öffentlichen Schlüssel mit anderen Personen aus.**

   Nach der Erzeugung eines Schlüsselpaars können Sie die Korrespondez mit anderen PGP-Benutzern beginnen. Sie benötigen dazu eine Kopie des öffentlichen Schlüssels der anderen Benutzer, die wiederum eine Kopie Ihres öffentlichen Schlüssels benötigen. Das Austauschen von Schlüsseln ist einfach, da Ihr öffentlicher Schlüssel nur aus einem Textblock besteht. Sie können Ihren öffentlichen Schlüssel in eine E-Mail-Nachricht einfügen, in eine Datei kopieren oder an einen öffentlichen oder firmeninternen Schlüsselserver senden, wo sich jeder bei Bedarf eine Kopie Ihres Schlüssels holen kann.

   Weitere Informationen zum Austauschen von öffentlichen Schlüsseln finden Sie im Abschnitt "Öffentliche Schlüssel mit anderen Personen austauschen" auf Seite 55.

4. **Überprüfen Sie die Echtheit der öffentlichen Schlüssel.**

   Wenn Sie die Kopie eines öffentlichen Schlüssels von einem anderen Benutzer erhalten haben, können Sie sie Ihrem öffentlichen Schlüsselbund hinzufügen. Vergewissern Sie sich, daß der Schlüssel nicht verfälscht wurde und daß er tatsächlich dem angegebenen Eigentümer gehört. Vergleichen Sie dazu den eindeutigen *Fingerabdruck* Ihrer Kopie des öffentlichen Schlüssels eines anderen Benutzers mit dem Fingerabdruck des Originalschlüssels dieser Person. Wenn Sie sicher sind, daß Sie über einen echten öffentlichen Schlüssel verfügen, unterschreiben Sie ihn. Dadurch geben Sie an, daß der Schlüssel Ihrer Meinung nach echt ist und verwendet werden kann. Außerdem können Sie dem Schlüsseleigentümer ein bestimmtes Maß an Vertrauen aussprechen. Damit geben Sie an, wieviel Vertrauen Sie dieser Person im Hinblick auf deren Verbürgung für die Echtheit des öffentlichen Schlüssels einer anderen Person entgegenbringen.

   Weitere Informationen zum Überprüfen Ihrer Schlüssel finden Sie im Abschnitt "Echtheit eines Schlüssels verifizieren" auf Seite 62.

5. **Beginnen Sie, Ihre E-Mail-Nachrichten und Dateien zu sichern.**

   Wenn Sie Ihr Schlüsselpaar erstellt und die öffentlichen Schlüssel ausgetauscht haben, können Sie mit dem Verschlüsseln, Unterschreiben, Entschlüsseln und Verifizieren Ihrer E-Mail-Nachrichten und Dateien beginnen.

   Wählen Sie dazu die Datei bzw. E-Mail aus, die Sie sichern möchten, und wählen Sie dann den gewünschten Befehl aus einem der PGP-Menüs (“Verschlüsseln”, “Unterschreiben”, “Entschlüsseln” oder “Überprüfen”). Die meisten Anwendungen verfügen über solche PGP-Menüs. Informationen dazu, wie Sie auf ein PGP-Menü zugreifen können, finden Sie in Kapitel 2, “Kurze Einführung in PGP”.

   Genaue Anweisungen zum Sichern Ihrer E-Mail-Nachrichten und Dateien finden Sie in ”Teil III: Dateien, E-Mail-Nachrichten und Instantnachrichten sichern”. Weitere Informationen zum Sichern Ihrer Netzwerkkommunikation erhalten Sie in ”Teil IV: Netzwerkkommunikation mit PGPnet sichern”.

6. **Bereinigen Sie Ihre Datenträger.**

   Wenn Sie eine Datei unwiederbringlich löschen möchten, können Sie mit der Funktion “Endgültig löschen” sicherstellen, daß die Datei nicht mehr wiederhergestellt werden kann. Die Datei wird sofort überschrieben, so daß sie auch nicht mehr mit einer Datenwiederherstellungssoftware wiederhergestellt werden kann.

   Weitere Informationen zum endgültigen Löschen von Dateien finden Sie im Abschnitt “Dateien unwiederbringlich löschen und Speicherplatz bereinigen” auf Seite 132.

Kurze Einführung in PGP 2

Wie Sie auf PGP zugreifen, hängt ganz davon ab, was zum entsprechenden Zeitpunkt gerade am günstigsten für Sie ist. PGP arbeitet mit den in anderen Anwendungen erstellten Daten. Daher sind die PGP-Funktionen in Abhängigkeit von den von Ihnen jeweils ausgeführten Vorgängen jederzeit sofort verfügbar.

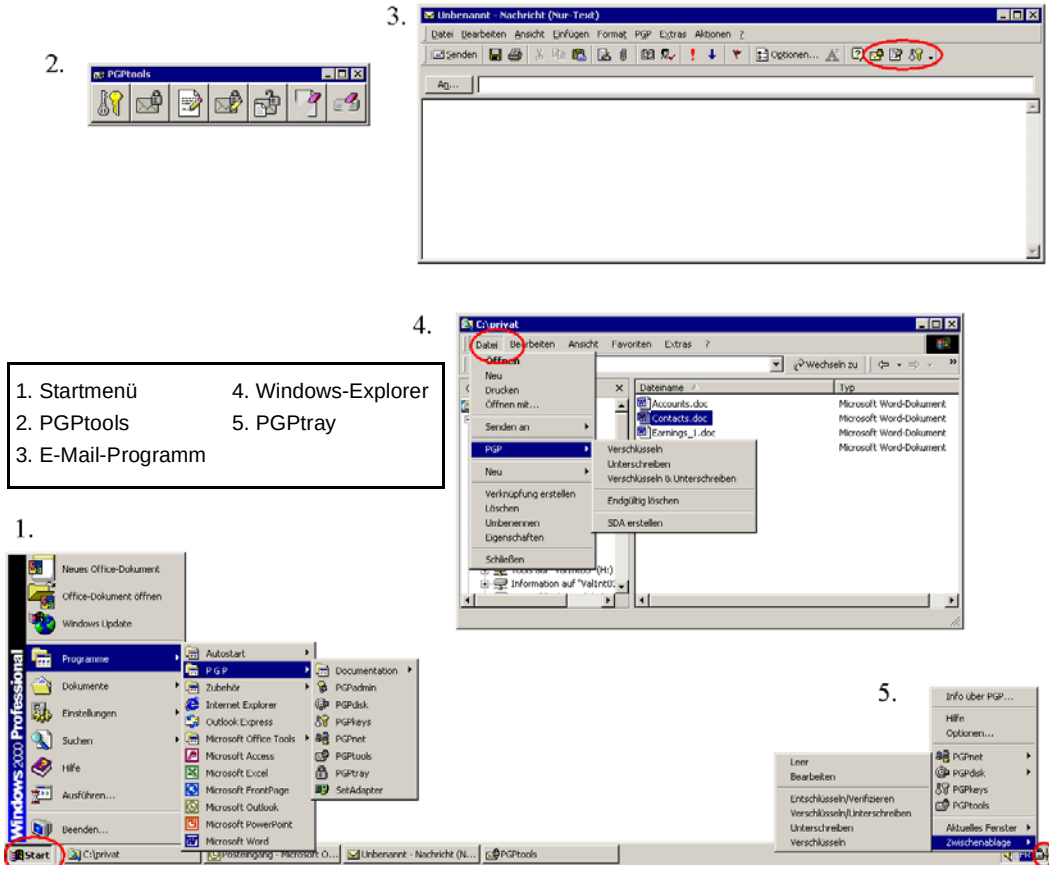


Abbildung 2-1. Zugriffsmöglichkeiten auf PGP

Startmenü

Viele der PGP-Dienstprogramme (PGPkeys, PGPtools, PGPtray und PGPdisk) können Sie (wie in Abbildung 2-1 unter der Nummer 1 dargestellt) vom Startmenü aus starten. Klicken Sie dazu in der Task-Leiste auf **Start**, zeigen Sie auf **Programme**, und klicken Sie auf **PGP**.

PGPtools

Wenn Sie ein E-Mail-Programm verwenden, für das es kein PGP-Plugin gibt, oder wenn Sie PGP-Funktionen von anderen Anwendungen aus ausführen möchten, können Sie PGPtools verwenden, um Nachrichten und Dateien zu verschlüsseln und zu unterschreiben, zu entschlüsseln und zu verifizieren sowie unwiederherstellbar zu löschen. PGPtools kann entweder (wie in Abbildung 2-1, unter der Nummer 2 dargestellt) über das Systemfeld der Task-Leiste (siehe Abbildung 2-1, Nummer 5) oder durch Klicken auf **Start—> Programme—>PGP—>PGPtools** geöffnet werden.

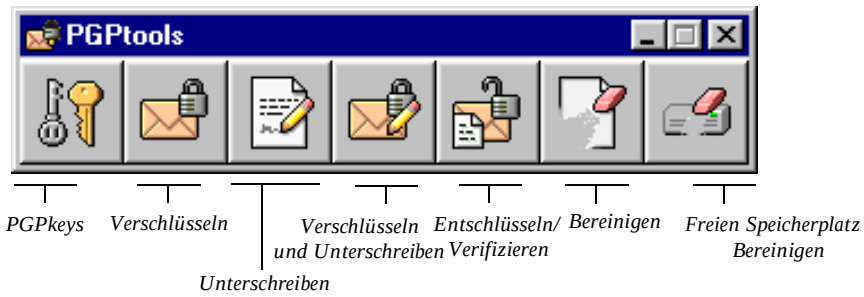


Abbildung 2-2. PGPtools

Möchten Sie Text oder Dateien verschlüsseln, entschlüsseln, unterschreiben oder verifizieren, markieren Sie den Text oder die Datei, und ziehen Sie sie in PGPtools auf die entsprechende Schaltfläche.

Wenn Sie mit Dateien arbeiten, klicken Sie in PGPtools auf die entsprechende Schaltfläche, um eine Datei auszuwählen, oder wählen Sie die Daten in der Zwischenablage aus.

Beim Entschlüsseln einer Datei wird ein “Speichern unter”-Dialogfeld geöffnet, und PGP erstellt eine neue Nur-Text-Datei mit der Erweiterung .txt; die verschlüsselte Datei wird mit der Erweiterung .txt.pgp versehen.

PGP-Plugins für E-Mail-Programme

PGP-Plugins sind für viele verbreitete E-Mail-Programme verfügbar. Mit diesen Plugins können die meisten der für das Erstellen und Lesen von E-Mails erforderlichen PGP-Operationen mit einem einfachen Mausklick direkt im E-Mail-Programm ausgeführt werden.

Auch wenn Sie mit einem E-Mail-Programm arbeiten, für das es kein PGP-Plugin gibt, können Sie den Nachrichtentext verschlüsseln bzw. entschlüsseln, indem Sie eines der anderen PGP-Dienstprogramme verwenden.

PGP verfügt über Plugins für die folgenden E-Mail-Programme:

- Qualcomm Eudora
- Microsoft Exchange
- Microsoft Outlook
- Microsoft Outlook Express
- Lotus Notes

Wenn ein PGP-Plugin installiert ist, werden in der Symbolleiste des E-Mail-Programms die Schaltflächen **Verschlüsseln** und **Entschlüsseln** angezeigt (siehe Abbildung 2-1 unter der Nummer 3). Wenn Sie auf die Schaltfläche mit dem Umschlag und dem Schloß ( ) klicken, wird Ihre Nachricht verschlüsselt, während Sie durch Klicken auf die Schaltfläche mit dem Stift und dem Papier ( ) angeben, daß Sie Ihre Nachricht unterschreiben möchten. Einige Programme verfügen außerdem über eine Schaltfläche, mit der Sie die Nachricht in einem Schritt verschlüsseln und unterschreiben können. Weitere Informationen zum Verwenden von PGP in E-Mail-Programmen finden Sie in Kapitel 5, “Sichere Kommunikation per E-Mail”.

PGP über den Windows-Explorers verwenden

Dateien wie beispielsweise Textverarbeitungsdokumente, Tabellen und Videoclips können Sie auch direkt über den Windows-Explorer verschlüsseln und unterschreiben bzw. entschlüsseln und verifizieren.

Wenn Sie vom Windows-Explorer aus auf die PGP-Funktionen zugreifen möchten, wählen Sie im Untermenü **PGP** des Menüs **Datei** die entsprechende Option (siehe Abbildung 2-1 unter der Nummer 4). Welche Optionen angezeigt werden, hängt vom aktuellen Status der ausgewählten Datei ab. Wenn die Datei noch nicht verschlüsselt oder unterschrieben wurde, werden im Menü die Optionen zum Verschlüsseln und Unterschreiben angezeigt. Wenn die Datei hingegen bereits verschlüsselt oder unterschrieben wurde, werden die Optionen zum Entschlüsseln und Verifizieren des Dateiinhalts angezeigt.

PGPtray

Auf viele der Hauptfunktionen von PGP können Sie zugreifen, indem Sie auf das graue Schloßsymbol ( ) klicken, das sich normalerweise im Systemfeld der Task-Leiste befindet (siehe Abbildung 2-1 unter der Nummer 5), und dann den entsprechenden Menübefehl wählen. (Wenn das Systemfeld der Task-Leiste kein Schloßsymbol enthält, starten Sie PGPtray vom Startmenü aus, bzw. lesen Sie im Abschnitt “Allgemeine Optionen festlegen” auf Seite 244 nach, wie weiter vorzugehen ist.) Auf diese Weise erhalten Sie unmittelbar Zugriff auf die PGP-Funktionen, gleich in welcher Anwendung Sie gerade arbeiten.

HINWEIS: Aus dem Aussehen des PGPtray-Symbols läßt sich erkennen, ob PGPnet deaktiviert oder nicht installiert (graues Schloß im Netzwerk) oder installiert, aber nicht aktiv ist (graues Schloß im Netzwerk mit rotem X). Wenn Sie PGPnet nicht installiert haben, erscheint im Systemfeld der Task-Leiste statt des PGPnet-Schloßsymbols das graue Schloßsymbol ( ). Weitere Informationen zu den Schloßsymbolen in PGPtray finden Sie im Abschnitt “Das PGPtray-Symbol” auf Seite 185.

PGPtray-Optionen “Zwischenablage” und “Aktuelles Fenster”

Wenn es für Ihr E-Mail-Programm kein PGP-Plugin gibt oder Sie mit Text arbeiten, der in einer anderen Anwendung erstellt wurde, können Sie die Funktionen zum Ver- und Entschlüsseln und zum Unterschreiben und Verifizieren über die Windows-Zwischenablage oder innerhalb des aktuellen Anwendungsfensters verwenden.

Über die Windows-Zwischenablage

Wenn Sie beispielsweise Text verschlüsseln oder mit einer Unterschrift versehen möchten, können Sie diesen mit STRG+C aus dem Textverarbeitungsprogramm in die Zwischenablage kopieren, ihn mit den entsprechenden PGP-Funktionen verschlüsseln und unterschreiben und den so bearbeiteten Text dann mit STRG+V wieder in das Textverarbeitungsprogramm einfügen, von wo aus er an die gewünschten Empfänger gesendet werden kann. Auch die Umkehrung ist möglich: Kopieren Sie den verschlüsselten (*chiffrierten*) Text aus Ihrem Programm in die Zwischenablage, entschlüsseln und verifizieren Sie die Daten, und schauen Sie sich dann den Inhalt an. Nach dem Lesen der entschlüsselten Nachricht können Sie entscheiden, ob Sie die Daten unverschlüsselt speichern oder in verschlüsselter Form aufbewahren möchten.

Innerhalb des aktuellen Fensters

Dieselben Verschlüsselungsaufgaben können Sie auch über die PGPtray-Menüoption **Aktuelles Fenster** ausführen, mit der der Text aus dem aktuellen Fenster in die Zwischenablage kopiert wird, wo dann die entsprechenden Vorgänge ausgeführt werden.

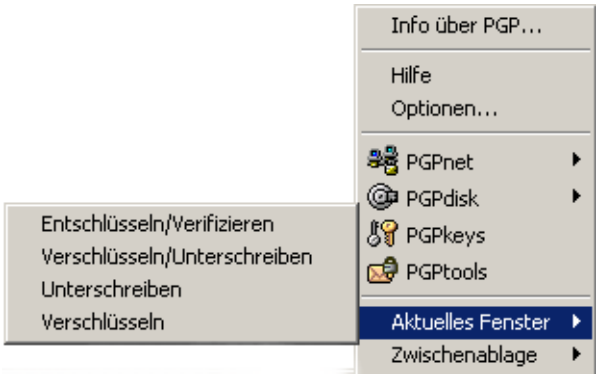


Abbildung 2-3. PGPtray-Option “Aktuelles Fenster”

Arbeit produktiver gestalten

Obwohl PGP recht einfach zu benutzen ist, gibt es eine Reihe von Möglichkeiten, die Ihnen helfen, Ihre Arbeit mit PGP noch produktiver zu gestalten. So können Sie beispielsweise beim Verwalten Ihrer Schlüssel im PGPkeys-Fenster durch Drücken der rechten Maustaste alle erforderlichen PGP-Funktionen aufrufen – der Weg über die Menüleiste entfällt. Sie können auch eine Datei mit einem Schlüssel in das PGPkeys-Fenster ziehen, um sie Ihrem Schlüsselbund hinzuzufügen.

Außerdem stehen für die meisten Menüoperationen auch Tastaturbefehle, sogenannte *Hotkeys*, zur Verfügung. Informationen zum Erstellen von PGP-Hotkeys finden Sie im Abschnitt “HotKey-Optionen festlegen” auf Seite 253.

Hilfe aufrufen

Wenn Sie die Option **Hilfe** in **PGPtray** oder im PGPkeys-Menü **Hilfe** wählen, wird das PGP-Hilfesystem geöffnet, in dem Sie einen allgemeinen Überblick über das Programm sowie Handlungsanweisungen finden. Viele Dialogfelder verfügen auch über eine kontextsensitive Hilfe, die durch Klicken auf das Fragezeichen in der oberen rechten Fensterecke und anschließendes Zeigen mit dem Cursor auf den betroffenen Bildschirmbereich aufgerufen werden kann. Daraufhin wird eine kurze Erklärung zum jeweiligen Bildschirmbereich angezeigt.

Teil II: Mit Schlüsseln arbeiten

- **Kapitel 3: Schlüssel erstellen und austauschen**
- **Kapitel 4: Schlüssel verwalten**

Schlüssel erstellen und austauschen 3

In diesem Kapitel wird beschrieben, wie Sie aus einem öffentlichen und einem privaten Schlüssel bestehende Schlüsselpaare erstellen, die Sie zur Kommunikation mit anderen PGP-Benutzern benötigen. Außerdem wird beschrieben, wie Sie Ihren öffentlichen Schlüssel verteilen und die öffentlichen Schlüssel von anderen erhalten, so daß Sie mit dem Austausch privater und authentifizierter E-Mail-Nachrichten beginnen können.

Begriffe und Konzepte im Zusammenhang mit Schlüsseln

PGP basiert auf einem allgemein anerkannten und sehr zuverlässigen *Verschlüsselungssystem mit öffentlichen Schlüsseln* (siehe Abbildung 3-1), mit dem Sie und andere PGP-Benutzer Schlüsselpaare erzeugen können, die jeweils aus einem *privaten* Schlüssel und einem *öffentlichen* Schlüssel bestehen.
Wie der Name schon sagt, haben nur Sie Zugriff auf Ihren privaten Schlüssel. Zur Kommunikation mit einem anderen PGP-Benutzer benötigt dieser jedoch eine Kopie Ihres öffentlichen Schlüssels, und Sie benötigen eine Kopie seines öffentlichen Schlüssels. Sie brauchen Ihren privaten Schlüssel zum Unterschreiben der E-Mail-Nachrichten und Dateianhänge, die Sie an andere senden, sowie zur Entschlüsselung der von anderen erhaltenen Nachrichten und Dateianhänge. Umgekehrt gilt dasselbe Prinzip: Sie verwenden die öffentlichen Schlüssel anderer Personen, um verschlüsselte E-Mail-Nachrichten an sie zu senden und um ihre digitalen Unterschriften zu verifizieren.

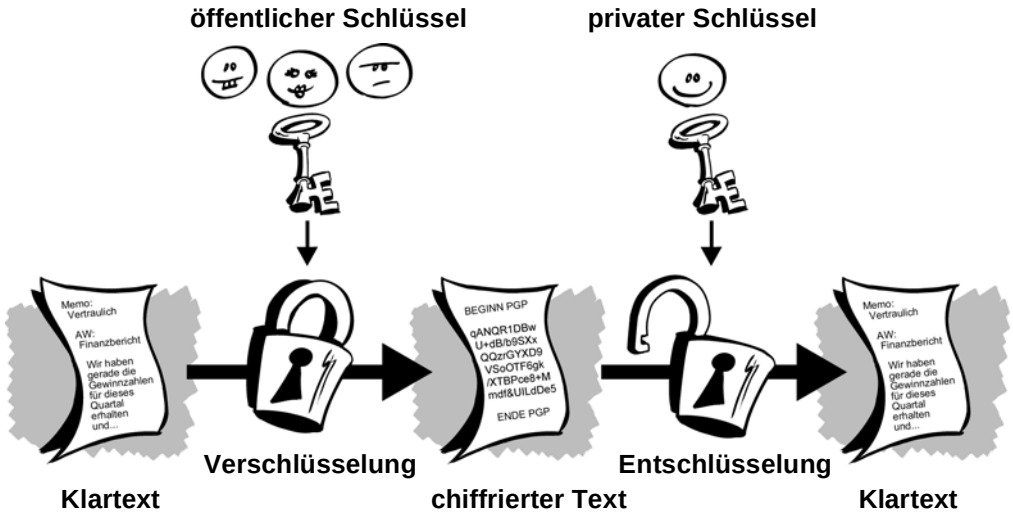


Abbildung 3-1. Kryptographie mit öffentlichen Schlüsseln

Schlüsselpaare erstellen

Wenn Sie diesen Schritt nicht bereits in einer älteren PGP-Version durchgeführt haben, müssen Sie zunächst ein neues Schlüsselpaar erstellen, bevor Sie verschlüsselte und unterschriebene E-Mail-Nachrichten senden oder empfangen können. In PGPkeys erzeugen Sie ein neues Schlüsselpaar mit Hilfe des PGP-Schlüsselerzeugungsassistenten, der Sie durch diesen Prozeß begleitet. Wenn Sie jedoch noch kein neues Schlüsselpaar erstellt haben, können Sie dies mit Hilfe des PGP-Schlüsselerzeugungsassistenten nachholen.

HINWEIS: Wenn Sie bereits ein Schlüsselpaar besitzen, legen Sie beim Ausführen der PGPkeys-Anwendung den Pfad für Ihre Schlüssel fest. Auf der Registerkarte **Dateien** des Dialogfelds **PGP-Optionen** können Sie jederzeit den Speicherort Ihrer Schlüsselbunddateien ermitteln.

WICHTIG: Auch wenn es durchaus Spaß macht, ein Schlüsselpaar zu erzeugen, sollten Sie nur dann mehr als ein solches Paar für sich erzeugen, wenn dies wirklich erforderlich ist. Wenn ein anderer Benutzer Ihnen eine E-Mail-Nachricht senden möchte, könnte er irritiert sein, wenn Sie mehr als ein Schlüsselpaar besitzen. Außerdem ist die Gefahr bei mehreren Schlüsselpaaren größer, daß Sie die jeweiligen Paßwörter durcheinander bringen oder ganz vergessen.

So erstellen Sie ein neues Schlüsselpaar:

1. Öffnen Sie PGPkeys. Dazu stehen Ihnen folgende Möglichkeiten zur Verfügung:

   - Klicken Sie auf **Start —> Programme —> PGP —> PGPkeys**.
   - Klicken Sie auf das PGPtray-Symbol ( ) im Systemfeld der Task-Leiste, und wählen Sie dann **PGPkeys**.
   - Klicken Sie auf in der Symbolleiste Ihrer E-Mail-Anwendung.

   Daraufhin wird das PGPkeys-Fenster geöffnet (Abbildung 3-2 auf Seite 43), in dem Ihre Schlüsselpaare sowie alle öffentlichen Schlüssel anderer Benutzer angezeigt werden, die Sie Ihrem öffentlichen Schlüsselbund hinzugefügt haben. Von diesem Fenster aus führen Sie zukünftig auch alle Schlüsselverwaltungsfunktionen aus.

HINWEIS: Je nach Situation ist das PGPkeys-Fenster (Abbildung 3-2) entweder leer oder so von Ihrem Administrator vorkonfiguriert, daß bestimmte Schlüssel angezeigt werden.

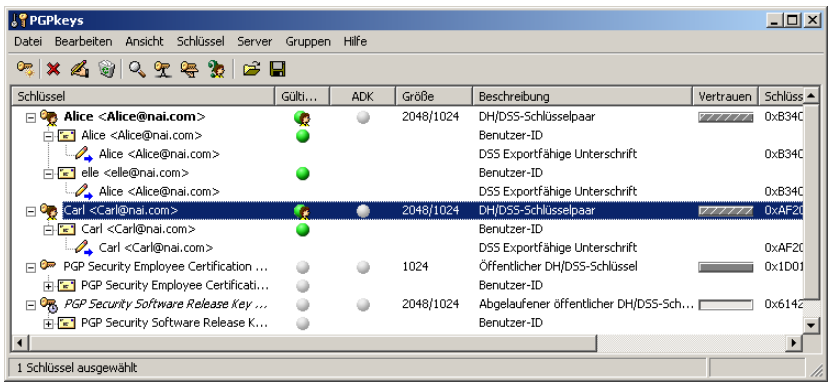


Abbildung 3-2. PGPkeys

2. Klicken Sie auf in der PGPkeys-Menüleiste.

   Der PGP-Schlüsselerzeugungsassistent zeigt im ersten Bildschirm einige einführende Informationen an.

3. Klicken Sie nach dem Lesen dieser Informationen auf **Weiter**, um zum nächsten Fenster zu wechseln.

   Wenn Sie einen benutzerdefinierten Schlüssel erstellen möchten, klicken Sie auf **Expert**. Sie können den Typ des zu erzeugenden Schlüssels auswählen, eine Schlüsselgröße festlegen und ein Ablaufdatum bestimmen. Wenn Sie einen benutzerdefinierten Schlüssel erstellen möchten, fahren Sie mit den in "So erzeugen Sie einen benutzerdefinierten Schlüssel:" auf Seite 46 beschriebenen Schritten fort.

   Sie werden vom PGP-Schlüsselerzeugungsassistenten dazu aufgefordert, Ihren Namen und Ihre E-Mail-Adresse einzugeben.

4. Geben Sie im Feld **Vollständiger Name** Ihren Namen und im Feld **E-Mail** Ihre E-Mail-Adresse ein.

   Die Eingabe Ihres tatsächlichen Namens bzw. Ihrer E-Mail-Adresse ist nicht unbedingt erforderlich. Durch die Verwendung Ihres tatsächlichen Namens ist es für andere Personen jedoch einfacher, Sie als den Eigentümer Ihres öffentlichen Schlüssels zu identifizieren. Indem Sie Ihre korrekte E-Mail-Adresse verwenden, können Sie und andere außerdem eine Plugin-Funktion nutzen, die den entsprechenden Schlüssel an Ihrem aktuellen Schlüsselbund automatisch sucht, wenn Sie eine E-Mail-Nachricht an einen bestimmten Empfänger adressieren. Es gibt aber auch *firmenweite Unterschriftenschlüssel* und *zusätzliche Entschlüsselungsschlüssel (ADKs)*, für die die Angabe von E-Mail-Adressen keine Bedeutung hat, weil sie nicht für Einzelpersonen stehen. Weitere Informationen zu firmenweiten Unterschriftenschlüsseln und ADKs finden Sie in *Einführung in die Kryptographie*.

5. Klicken Sie auf **Weiter**, um fortzufahren.

   Sie werden vom Schlüsselerzeugungsassistenten dazu aufgefordert, eine Paßphrase einzugeben.

6. Geben Sie im Dialogfeld **Paßphrase** die Folge von Zeichen oder Wörtern ein, die Sie zur Gewährleistung des exklusiven Zugangs zu Ihrem persönlichen Schlüssel verwenden möchten. Drücken Sie zur Bestätigung Ihrer Eingabe die TABULATORTASTE, um zur nächsten Zeile zu gelangen. Geben Sie hier Ihre Paßphrase nochmals ein.

   Um zusätzliche Sicherheit zu gewährleisten, werden die von Ihnen eingegebenen Zeichen für die Paßphrase normalerweise nicht auf dem Bildschirm angezeigt. Wenn Sie sich jedoch sicher sind, unbeobachtet zu sein, und die Zeichen Ihrer Paßphrase bei der Eingabe sehen möchten, deaktivieren Sie die Option **Eingabe verbergen**.

HINWEIS: Ihre Paßphrase sollte aus mehreren Wörtern bestehen und kann Leerzeichen, Ziffern und Satzzeichen enthalten. Denken Sie sich etwas aus, das Sie sich leicht merken, andere aber nicht erraten können. Bei der Paßphrase müssen Sie auf die Groß- und Kleinschreibung achten. Je länger Ihre Paßphrase und je größer die Verschiedenheit der in ihr enthaltenen Zeichen ist, desto sicherer ist sie. In komplizierten Paßphrasen sind Groß- und Kleinbuchstaben, Ziffern, Satzzeichen und Leerzeichen enthalten. Solche Paßphrasen werden aber auch leichter vergessen. Weitere Informationen zur Auswahl einer Paßphrase finden Sie im Abschnitt "Einprägsame Paßphrasen erstellen" auf Seite 49.

WARNUNG: Sofern Ihr Administrator keine Möglichkeiten zur Rekonstruktion von PGP-Schlüsseln für Ihr Unternehmen eingerichtet hat, ist niemand (auch Network Associates nicht) in der Lage, Schlüssel, deren Paßphrase Sie vergessen haben, zu retten.

7. Klicken Sie auf **Weiter**, um mit der Schlüsselerzeugung zu beginnen.

   Der PGP-Schlüsselerzeugungsassistent zeigt an, daß Ihr Schlüssel gerade erzeugt wird.

   Wenn Sie eine unpassende Paßphrase eingegeben haben, wird vor der Erzeugung der Schlüssel eine Warnmeldung angezeigt, und Sie können nun entweder die ungeeignete Paßphrase akzeptieren oder eine sicherere Paßphrase eingeben, bevor Sie weitermachen. Weitere Informationen zu Paßphrasen finden Sie im Abschnitt "Einprägsame Paßphrasen erstellen" auf Seite 49.

   Ihre Mausbewegungen und Tastatureingaben erzeugen Zufallsinformationen, die für das Erzeugen eines eindeutigen Schlüsselpaares benötigt werden. Wenn nicht genügend Zufallswerte für die Erstellung des Schlüssels zur Verfügung stehen, wird das **PGP-Dialogfeld zur Erzeugung von Zufallswerten** angezeigt. Bewegen Sie die Maus wie im Dialogfeld beschrieben, und drücken Sie eine beliebige Folge von Tasten, bis die Statusleiste vollständig ausgefüllt ist.

HINWEIS: PGPkeys sammelt fortlaufend Zufallswerte aus vielen Quellen im System, einschließlich Mausposition, Zeitabständen und Tastenanschlägen. Wenn das **PGP-Dialogfeld zur Erzeugung von Zufallswerten** nicht angezeigt wird, bedeutet dies, daß PGP bereits alle benötigten Informationen zur Erzeugung eines Schlüsselpaares gesammelt hat.

Nachdem die Schlüsselerstellung gestartet wurde, kann es einige Zeit dauern, bis die Schlüssel erzeugt sind.

Wenn der Schlüsselerzeugungsprozeß abgeschlossen ist, wird das letzte Fenster angezeigt.

8. Klicken Sie auf **Fertig stellen**. PGP fügt automatisch dem privaten Schlüsselbund Ihren privaten Schlüssel und dem öffentlichen Schlüsselbund Ihren öffentlichen Schlüssel hinzu.

Nachdem Sie ein Schlüsselpaar erzeugt haben, können Sie mit PGPkeys weitere neue Schlüsselpaare erstellen und Ihre übrigen Schlüssel verwalten. So können Sie beispielsweise die mit einem bestimmten Schlüssel verbundenen Attribute überprüfen und angeben, inwieweit Sie darauf vertrauen, daß der Schlüssel tatsächlich dem angegebenen Eigentümer gehört, und ob diese Person zuverlässig genug ist, sich für die Echtheit der Schlüssel anderer Benutzer zu verbürgen. Ausführliche Informationen zu den Schlüsselverwaltungsfunktionen, die Sie im PGPkeys-Fenster ausführen können, finden Sie in Kapitel 4.

So erzeugen Sie einen benutzerdefinierten Schlüssel:

1. Führen Sie die in “So erstellen Sie ein neues Schlüsselpaar:” auf Seite 43 genannten Schritte 1 und 2 aus.

2. Klicken Sie im Begrüßungsbildschirm des **Schlüsselerzeugungsassistenten** auf **Expert**, und wählen Sie den Schlüsseltyp, die Schlüsselgröße und/oder ein Ablaufdatum aus.

   Der Bildschirm **Expert-Modus zur Auswahl der Schlüsselparameter** des Schlüsselerzeugungsassistenten wird geöffnet (siehe Abbildung 3-3).

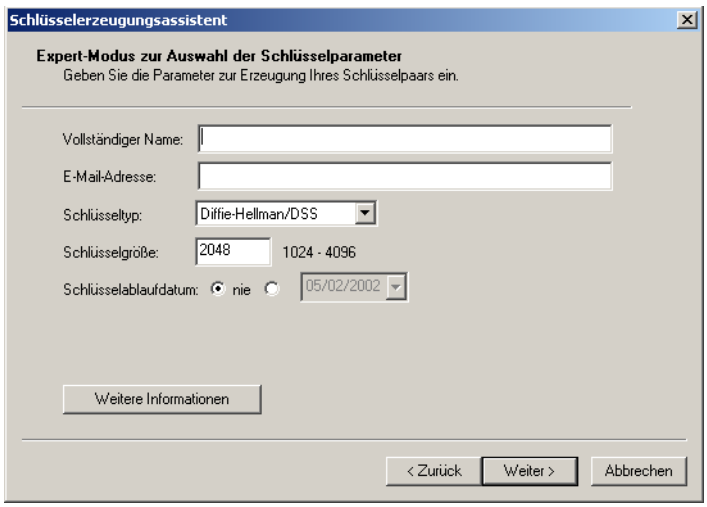


Abbildung 3-3. Schlüsselerzeugungsassistent (Registerkarte “Expert”)

3. Wählen Sie im Feld **Schlüsseltyp** einen Schlüsseltyp aus**.**

Wählen Sie die Option **Diffie-Hellman/DSS**, wenn Sie von möglichst vielen PGP-Schlüsselfunktionen profitieren möchten, wie beispielsweise der Verwendung zusätzlicher Entschlüsselungsschlüssel (ADKs) und zugeordneter Rücknahmeschlüssel, der Aufteilung von Schlüsseln in mehrere Verschlüsselungsteilschlüssel sowie vom Einsatz von Foto-IDs.

Wählen Sie die Option **RSA** bzw. **RSA Legacy**, wenn Sie mit Personen korrespondieren möchten, die RSA-Schlüssel verwenden.

Das RSA-Schlüsselformat unterstützt die Verwendung zusätzlicher PGP-Entschlüsselungsschlüssel (ADKs), zugeordneter Rücknahmeschlüssel und mehrerer Verschlüsselungsteilschlüssel sowie die Foto-ID-Funktionen. Bisher standen diese Funktionen nur Benutzern von Diffie-Hellman-Schlüsseln zur Verfügung. PGP unterstützt auch weiterhin Benutzer mit RSA-Schlüsseln im alten Schlüsselformat (diese werden jetzt als “RSA Legacy”-Schlüssel bezeichnet).

WICHTIG: Der Schlüsseltyp “RSA” ist in vollem Umfang nur mit den PGP-Versionen 7.0 und höher und anderen OpenPGP-Anwendungen kompatibel.

Das Schlüsselformat “RSA Legacy” sollten Sie nur wählen, wenn diejenigen, mit denen Sie kommunizieren, ältere Versionen von PGP verwenden. Ist dies nicht der Fall, wählen Sie das neue RSA-Schlüsselformat. RSA Legacy-Schlüssel unterstützen viele der neueren PGP-Schlüsselfunktionen nicht.

4. Klicken Sie auf **Weiter**.
5. Legen Sie im Feld **Schlüsselgröße** eine Schlüsselgröße zwischen 1024 und 4096 Bits für Diffie-Hellman / DSS-Schlüssel bzw. 1024 und 2048 für RSA-Schlüssel fest.

HINWEIS: Die Erzeugung eines großen Schlüssels nimmt je nach Leistungsfähigkeit Ihres Rechners möglicherweise mehr Zeit in Anspruch.

Die Schlüsselgröße entspricht der Bitanzahl, die zum Erzeugen des digitalen Schlüssels benötigt wird. Je größer der Schlüssel ist, desto geringer ist die Gefahr, daß er von jemandem dekodiert wird. Allerdings wird mehr Zeit für das Entschlüsseln und Verschlüsseln benötigt. Sie müssen also zwischen einer schnelleren Durchführung der PGP-Funktionen, gewährleistet durch einen kleineren Schlüssel, und einer höheren Sicherheitsebene durch einen größeren Schlüssel wählen. Normalerweise ist ein Schlüssel mit 1024 Bit sicher genug. Ein größerer Schlüssel ist nur dann erforderlich, wenn die auszutauschenden Daten extrem wichtig und vertraulich und für Dritte von so großem Interesse sind, daß sich kosten- und zeitaufwendige kryptographische Anstrengungen zu seiner Dekodierung lohnen würden.

HINWEIS: Bei der Erstellung eines Diffie-Hellman / DSS-Schlüsselpaares ist die Größe des DSS-Anteils des Schlüssels kleiner oder gleich der Größe des Diffie-Hellman-Anteils des Schlüssels und auf eine maximale Größe von 1024 Bit begrenzt.

---

6. Geben Sie das Datum an, ab dem Ihre Schlüssel ihre Gültigkeit verlieren sollen. Verwenden Sie die Standardeinstellung **nie**, wenn sie niemals ungültig werden sollen, oder geben Sie ein bestimmtes Datum ein, nach dem Ihre Schlüssel ihre Gültigkeit verlieren werden.

   Wenn Sie ein Schlüsselpaar erstellen und Ihren öffentlichen Schlüssel an alle Personen verteilt haben, mit denen Sie korrespondieren, verwenden Sie von diesem Zeitpunkt an wahrscheinlich immer dieselben Schlüssel. Unter bestimmten Umständen möchten Sie jedoch möglicherweise ein spezielles Schlüsselpaar nur für einen begrenzten Zeitraum verwenden. In einem solchen Fall kann der öffentliche Schlüssel, wenn dessen Gültigkeit abgelaufen ist, zwar nicht mehr von anderen zum Verschlüsseln von Nachrichten an Sie verwendet werden, Ihre digitale Unterschrift kann jedoch damit noch überprüft werden. Umgekehrt gilt, daß Ihr privater Schlüssel auch dann noch zum Entschlüsseln von an Sie gesendeten Nachrichten verwendet werden kann, wenn dessen Gültigkeit abgelaufen ist, die Nachrichten aber vor Ablauf der Gültigkeit des öffentlichen Schlüssels gesendet wurden. Zum Unterzeichnen von Nachrichten an andere kann er aber nicht mehr verwendet werden.

7. Führen Sie Schritt 6 bis Schritt 8 auf Seite 44 aus, um die Schlüsselerzeugung abzuschließen.

   Im PGPkeys-Fenster wird ein Schlüsselpaar angezeigt, das Ihre neu erstellten Schlüssel darstellt. Jetzt können Sie Ihre Schlüssel näher untersuchen, indem Sie ihre Eigenschaften und Attribute überprüfen. Sie können nun auch andere E-Mail-Adressen hinzufügen. Nähere Informationen zum Bearbeiten der Informationen Ihres Schlüsselpaares finden Sie im Abschnitt “Eigenes Schlüsselpaar ändern” auf Seite 50.

Einprägsame Paßphrasen erstellen

Wenn Sie einmal eine Datei verschlüsselt haben und dann später feststellen mußten, daß Sie sie nicht wieder entschlüsseln konnten, werden Sie wissen, wie wichtig es ist, eine einprägsame Paßphrase zu wählen. Die meisten Anwendungen verlangen lediglich ein Paßwort, das aus einem Wort mit drei bis acht Zeichen besteht. Aus verschiedenen Gründen empfehlen wir jedoch, nicht nur ein Wort als Paßphrase zu verwenden. Ein Einwort-Paßwort ist anfällig für einen “Wörterbuchangriff”, welcher darin besteht, einen Computer alle Wörter im Wörterbuch durchprobieren zu lassen, bis Ihr Paßwort gefunden wird. Zum Schutz gegen diese Art des Angriffs werden im allgemeinen Paßwörter aus einer Kombination von Groß- und Kleinbuchstaben, Zahlen, Satz- und Leerzeichen empfohlen. Dadurch kommt ein komplizierteres Paßwort zustande, das aber unverständlich und daher leichter zu vergessen ist.

Das willkürliche Einfügen einer Menge nichtalphabetischer Zeichen zur Vereitelung eines solchen “Wörterbuchangriffs” führt zu einer leicht zu vergessenden Paßphrase. Wenn Sie Ihre Paßphrase aber vergessen, kann daraus wiederum ein verhängnisvoller Informationsverlust resultieren, da Sie in diesem Fall Ihre eigenen Dateien nicht mehr entschlüsseln können. Eine aus mehreren Wörtern bestehende Paßphrase ist aber weniger anfällig für einen “Wörterbuchangriff”. Es ist jedoch unwahrscheinlich, daß Sie sich die Paßphrase wortwörtlich merken können, es sei denn, die von Ihnen gewählte Paßphrase ist sehr einprägsam. Wenn Sie einer plötzlichen Eingebung folgend eine Zeile auswählen, ist es eher wahrscheinlich, daß Sie sie vergessen. Wählen Sie statt dessen etwas, was Sie ohnehin schon im Langzeitgedächtnis “gespeichert” haben. Verwenden Sie jedoch keine Wendung, die Sie in letzter Zeit jemandem gegenüber verwendet haben und auch kein berühmtes Zitat, da Ihre Paßphrase für einen raffinierten Hacker ja schwer zu erraten sein soll. Wenn die gewählte Wendung schon tief in Ihrem Langzeitgedächtnis verwurzelt ist, werden Sie sie wahrscheinlich nicht vergessen.

Wenn Sie jedoch so leichtsinnig sind, Ihre Paßphrase aufzuschreiben und an Ihren Monitor oder in Ihre Schreibtischschublade zu kleben, ist es ziemlich egal, was für eine Paßphrase Sie wählen.

Eigenes Schlüsselpaar ändern

Nachdem Sie einen Schlüssel erstellt haben, können Sie Ihrem Schlüsselpaar jederzeit eine Reihe von Elementen hinzufügen, Elemente entfernen bzw. diese ändern. Der folgenden Tabelle können Sie entnehmen, wo Sie Informationen zu den jeweiligen Aufgaben finden.

Aufgabe	Siehe
Foto-ID hinzufügen	“Foto-IDs zu Schlüsseln hinzufügen” auf Seite 83
zusätzliche Teilschlüssel hinzufügen	“Neue Teilschlüssel erstellen” auf Seite 85
neuen Benutzernamen und neue E-Mail-Adresse hinzufügen	“Neue Benutzernamen und Adressen einem Schlüsselpaar hinzufügen” auf Seite 82
Unterschriften hinzufügen bzw. entfernen	“Schlüssel oder Unterschriften aus Ihrem PGP-Schlüsselbund löschen” auf Seite 74
eigene Paßphrase ändern	“Eigene Paßphrase ändern” auf Seite 81
zugeordnete Rücknahmeschlüssel hinzufügen	“Zugeordneten Rücknahmeschlüssel festlegen” auf Seite 88

Aufgabe	Siehe
X.509-Zertifikat hinzufügen	“PGP-Schlüsseln X.509-Zertifikate hinzufügen” auf Seite 91
Schlüssel in mehrere Teile aufteilen	“Schlüssel teilen und wieder zusammensetzen” auf Seite 96

Sicherungskopien Ihrer Schlüssel erstellen

Wenn Sie ein Schlüsselpaar erzeugt haben, sollten Sie eine Kopie erstellen und diese an einem sicheren Ort aufbewahren, damit sie zur Verfügung steht, falls die Verwendung des Originalpaares einmal nicht möglich sein sollte. Beim Schließen von PGPkeys nach der Erstellung eines neuen Paares werden Sie von PGP aufgefordert, eine Sicherungskopie des Paares zu erstellen.

Ihre privaten und Ihre öffentlichen Schlüssel werden in separaten Schlüsselbunddateien gespeichert. Sie können diese an einen anderen Speicherort auf Ihrer Festplatte oder auf eine Diskette kopieren. Standardmäßig werden der private Schlüsselbund (SECRING.SKR) und der öffentliche Schlüsselbund (PUBRING.PKR) in Ihrem Ordner **Profile** gespeichert. Sie können die Sicherungskopien jedoch auch in einem anderen Pfad speichern.

Sie können PGP so konfigurieren, daß Ihre Schlüsselbunde beim Schließen von PGP automatisch gesichert werden. Die Optionen für das Sichern Ihrer Schlüsselbunde können Sie auf der Registerkarte **Erweitert** des Dialogfelds “PGP-Optionen” festlegen. Weitere Informationen dazu finden Sie in “Erweiterte Optionen festlegen” auf Seite 259.

Eigene Schlüssel schützen

Neben dem Erstellen von Sicherungskopien für Ihre Schlüssel sollten Sie Ihren privaten Schlüssel an einer besonders sicheren Stelle speichern. Obwohl Ihr privater Schlüssel durch eine Paßphrase geschützt ist, die nur Sie kennen sollten, ist es möglich, daß jemand Ihre Paßphrase entdeckt und dann mit Ihrem privaten Schlüssel Ihre E-Mail-Nachrichten entziffert oder Ihre digitale Unterschrift fälscht. Ihnen könnte beispielsweise jemand über die Schulter schauen und sehen, welche Tasten Sie drücken, oder er könnte die entsprechenden Signale auf dem Netzwerk oder sogar über das Internet abfangen.

Um zu verhindern, daß Dritte, die Ihre Paßphrase möglicherweise abgefangen haben, Ihren privaten Schlüssel verwenden, sollten Sie Ihren privaten Schlüssel ausschließlich auf Ihrem eigenen Computer speichern. Wenn Ihr Rechner an ein Netzwerk angeschlossen ist, müssen Sie sich auch vergewissern, daß Ihre Dateien nicht durch eine Sicherung durch Kopieren für das gesamte System automatisch erfaßt werden, wodurch andere Personen Zugang zu Ihrem privaten Schlüssel erhalten könnten. Angesichts dessen, wie einfach es ist, über Netzwerke auf Computer zuzugreifen, ist es bei der Arbeit mit streng vertraulichen Informationen empfehlenswert, Ihren privaten Schlüssel auf einer Diskette zu speichern, die Sie ähnlich wie einen herkömmlichen Schlüssel nur dann verwenden, wenn Sie private Informationen lesen oder unterschreiben möchten.

Als weitere Sicherheitsmaßnahme können Sie Ihrer privaten Schlüsselbunddatei einen anderen Namen zuweisen und sie an einer anderen Stelle als im Standardordner von PGP speichern. Auf der Registerkarte **Dateien** des Dialogfelds “PGP-Optionen” von **PGPkeys** können Sie Namen und Speicherorte für Ihre privaten und öffentlichen Schlüsselbunddateien festlegen.

Was passiert, wenn ich meine Paßphrase vergesse oder meinen Schlüssel verliere?

Wenn Sie Ihren Schlüssel verlieren oder Ihre Paßphrase vergessen und keine Kopie angelegt haben, aus der Sie Ihren Schlüssel wiederherstellen können, gibt es für Sie keine Möglichkeit mehr, jemals wieder die mit Ihrem Schlüssel verschlüsselten Informationen zu entschlüsseln. Sie können Ihren Schlüssel aber rekonstruieren, falls Ihr Administrator für Ihr Unternehmen die PGP-Schlüsselrekonstruktion implementiert hat. Bei der PGP-Schlüsselrekonstruktion wird Ihr Schlüssel auf einem PGP-Schlüsselrekonstruktionsserver verschlüsselt und gespeichert.

Was versteht man unter “PGP-Schlüsselrekonstruktion”?

Ihr Administrator kann einen PGP-Schlüsselrekonstruktionsserver einrichten, der als eine Art Sicherheitsnetz fungiert, falls Sie Ihren privaten Schlüssel oder Ihre Paßphrase vergessen bzw. anderweitig verlieren. Der Rekonstruktionsserver speichert Ihren Schlüssel, dies aber nur so, daß außer Ihnen keiner darauf zugreifen kann. Ihr Unternehmen ist nicht in der Lage, Ihren Schlüssel zu entschlüsseln.

Wenn Ihr Administrator die Schlüsselrekonstruktion als Teil der Sicherheitspolitik Ihres Unternehmens eingerichtet hat, werden Sie aufgefordert, zusätzliche “geheime” Informationen einzugeben, wenn Sie Ihr PGP-Schlüsselpaar erstellen bzw. wenn Sie die Option **Senden an Schlüsselrekonstruktionsserver** im **PGPkeys**-Menü **Server** wählen. Unter Umständen erhalten Sie von Ihrem Administrator auch eine Benutzer-ID und ein Paßwort, mit denen Sie sich beim Schlüsselrekonstruktionsserver anmelden können.

Wenn sich Ihr Schlüssel auf dem Server befindet, können Sie ihn mit Hilfe der Option **Schlüssel rekonstruieren** im PGPkeys-Menü **Schlüssel** jederzeit wiederherstellen. Informationen, wie Sie beim Rekonstruieren Ihres Schlüssels vorgehen müssen, finden Sie im Abschnitt “Schlüssel rekonstruieren” auf Seite 107.

So senden Sie Ihren Schlüssel an den Schlüsselrekonstruktionsserver Ihres Unternehmens:

1. Wenn sich beim Erstellen eines Schlüsselpaares das Dialogfeld **Schlüsselrekonstruktion** automatisch geöffnet hat, fahren Sie mit Schritt 3 fort. Andernfalls öffnen Sie PGPkeys, und wählen Sie Ihr Schlüsselpaar aus.
2. Öffnen Sie das Menü **Server/Senden an**, und wählen Sie die Option **Rekonstruktionsserver**.

   Das Dialogfeld **Schlüsselrekonstruktion** wird geöffnet (siehe Abbildung 3-4).

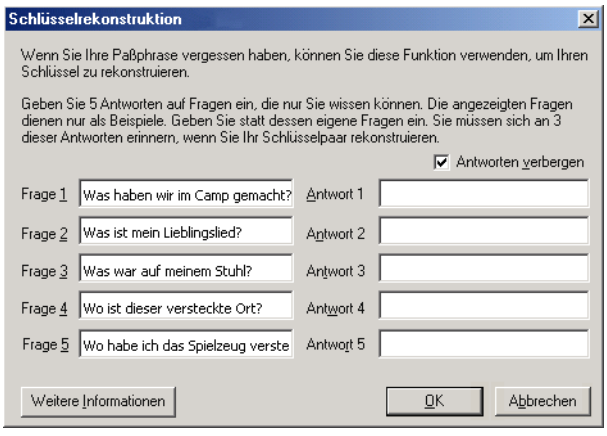


Abbildung 3-4. Dialogfeld “Schlüsselrekonstruktion”

3. Geben Sie in den **Fragefeldern** des Dialogfelds **Schlüsselrekonstruktion** (siehe Abbildung 3-4) fünf Fragen ein, die nur Sie beantworten können (bei den Standardfragen handelt es sich lediglich um Beispiele). Wählen Sie nicht offensichtliche persönliche Fragen, deren Antworten Sie sich gut merken können. Ihre Fragen können aus bis zu 95 Zeichen bestehen.

   Beispiele für geeignete Fragen sind “Mit wem war ich am Strand?” oder “Warum hat Fred mich verlassen?”.

   Ungeeignete Fragen sind zum Beispiel: “Wie lautet der Mädchenname meiner Mutter?” oder “Wo habe ich studiert?”.

   HINWEIS: Sie können, wenn Ihnen dies lieber ist, die Fragefelder auch leer lassen und einfach nur fünf Antworten eingeben.

   ---

4. Geben Sie in den **Antwortfeldern** die Antworten auf die entsprechenden Fragen ein. Bei der Eingabe Ihrer Antworten müssen Sie auf die Groß- und Kleinschreibung achten. Die Anzahl der Zeichen ist auf 255 begrenzt.

   Über die Option **Antworten verbergen** können Sie steuern, ob Ihre Antworten ein- oder ausgeblendet werden sollen.

5. Klicken Sie auf **OK**, um fortzufahren.

   Wenn das Dialogfeld **PGP – Eingabe der Paßphrase für Schlüssel** angezeigt wird, geben Sie die Paßphrase für Ihren Schlüssel ein, und klicken Sie auf **OK**.

   Wenn Sie aufgefordert werden, die **Benutzer-ID und das Paßwort für den Server** einzugeben, geben Sie zum Anmelden beim Server Ihre Benutzer-ID und das Paßwort ein. Wenn Sie Ihre ID bzw. Ihr Paßwort nicht kennen, wenden Sie sich an Ihren Administrator.

6. Klicken Sie auf **OK**.

   Ihr privater Schlüssel wird dann mit dem Blakely-Shamir-Schlüsselaufteilungsverfahren in fünf Teile aufgeteilt. Zum Rekonstruieren des Schlüssels werden drei dieser fünf Teile benötigt. Jedes Teil wird dann mit dem *Hash*, der eindeutigen Identifizierungsnummer einer Antwort, verschlüsselt. Wenn Sie drei der Fragen richtig beantworten können, sind Sie in der Lage, den ganzen Schlüssel erfolgreich zu rekonstruieren. Informationen dazu, wie Sie beim Rekonstruieren Ihres Schlüssels vorgehen müssen, finden Sie im Abschnitt “Schlüssel rekonstruieren” auf Seite 107.

Öffentliche Schlüssel mit anderen Personen austauschen

Nachdem Sie Ihre Schlüssel erstellt haben, müssen Sie sie mit den Personen austauschen, mit denen Sie kommunizieren möchten. Sie müssen Ihren öffentlichen Schlüssel anderen zur Verfügung stellen, damit diese verschlüsselte Daten an Sie senden und Ihre digitale Unterschrift verifizieren können. Zum Verschlüsseln Ihrer Nachrichten oder Dateien benötigen Sie eine Kopie der Schlüssel Ihres Kommunikationspartners. Ihr öffentlicher Schlüssel besteht im Prinzip aus einem Textblock. Daher ist es ziemlich einfach, ihn auf einem öffentlichen Schlüsselserver zugänglich zu machen, in eine E-Mail-Nachricht einzufügen oder ihn in eine Datei zu exportieren bzw. zu kopieren. Der Empfänger kann dann auf eine beliebige Art Ihren öffentlichen Schlüssel zu seinem öffentlichen Schlüsselbund hinzufügen.

Eigenen öffentlichen Schlüssel weitergeben

Für die Weitergabe Ihres öffentlichen Schlüssels stehen Ihnen drei Möglichkeiten zur Verfügung:

- Sie können Ihren öffentlichen Schlüssel über einen öffentlichen Schlüsselserver bereitstellen.
- Sie können Ihren öffentlichen Schlüssel in einer E-Mail-Nachricht versenden.
- Sie können Ihren öffentlichen Schlüssel in eine Textdatei exportieren bzw. kopieren und diese Datei weitergeben.

Eigenen öffentlichen Schlüssel auf einem Schlüsselserver ablegen

Der beste Weg, Ihren öffentlichen Schlüssel an andere weiterzugeben, besteht darin, ihn auf einem öffentlichen Schlüsselserver abzulegen. Ein öffentlicher Schlüsselserver ist eine große Datenbank mit Schlüsseln, über die jedermann auf die öffentlichen Schlüssel anderer zugreifen kann. Auf diese Weise können andere Personen verschlüsselte E-Mail-Nachrichten an Sie senden, ohne Sie extra um eine Kopie Ihres Schlüssels bitten zu müssen. Es ist dann auch nicht mehr notwendig, daß Sie und andere Benutzer eine Vielzahl öffentlicher Schlüssel verwalten, die Sie nur selten verwenden. Es gibt weltweit eine ganze Reihe von Schlüsselservern, u. a. die von Network Associates, Inc., auf denen Sie Ihren Schlüssel der Allgemeinheit zugänglich machen können. Wenn Sie PGP in einer Unternehmensumgebung verwenden, wird Ihr Administrator normalerweise die Einstellungen für Ihren Schlüsselserver vorkonfigurieren, so daß Sie sich um nichts mehr kümmern müssen.

Wenn Sie mit einem öffentlichen Schlüsselserver arbeiten (z. B. keyserver.pgp.com), sollten Sie vor dem Senden Ihres Schlüssels folgendes bedenken.

- Handelt es sich dabei um den Schlüssel, den Sie verwenden wollen? Wenn andere Benutzer mit Ihnen kommunizieren möchten, könnten diese wichtige Informationen mit diesem Schlüssel verschlüsseln. Wir empfehlen daher dringend, nur solche Schlüssel auf einen Schlüsselserver zu legen, die andere Benutzer auch verwenden sollen.
- Werden Sie sich an die Paßphrase für diesen Schlüssel erinnern, so daß Sie mit ihm verschlüsselte Daten abrufen können bzw. den Schlüssel zurücknehmen können, falls Sie ihn nicht verwenden möchten?
- Wenn ein Schlüssel einmal auf einem Schlüsselserver ist, bleibt er im allgemeinen auch dort. Es gibt nämlich eine Reihe von öffentlichen Schlüsselservern, auf denen das Löschen von Schlüsseln nicht möglich ist. Andere Server besitzen Replikationsfunktionen, die Schlüssel zwischen Schlüsselservern replizieren, so daß der Schlüssel selbst dann, wenn Sie Ihren Schlüssel von einem Server löschen können, aller Wahrscheinlichkeit nach woanders wieder auftaucht.

So senden Sie Ihren öffentlichen Schlüssel an einen Schlüsselserver:

1. Stellen Sie eine Verbindung zum Internet her.
2. Öffnen Sie PGPkeys.
3. Wählen Sie den öffentlichen Schlüssel aus, den Sie auf den Schlüsselserver kopieren möchten.
4. Öffnen Sie das **Server**-Menü, und wählen Sie dann im Untermenü **Senden an** den Schlüsselserver aus, auf dem Ihr Schlüssel abgelegt werden soll. (Der Schlüsselserver von Network Associates hat die Adresse http://certserver.pgp.com.) PGP informiert Sie darüber, wenn die Schlüssel erfolgreich auf dem Server abgelegt werden konnten.

Nachdem Sie eine Kopie Ihres öffentlichen Schlüssels auf einem Schlüsselserver abgelegt haben, steht er allen zur Verfügung, die Ihnen verschlüsselte Daten senden oder Ihre digitale Unterschrift verifizieren möchten. Selbst wenn Sie die betreffenden Personen nicht ausdrücklich auf Ihren öffentlichen Schlüssel hinweisen, können diese eine Kopie Ihres öffentlichen Schlüssels anfertigen, indem sie den Schlüsselserver nach Ihrem Namen oder Ihrer E-Mail-Adresse durchsuchen. Viele fügen die Web-Adresse für ihren öffentlichen Schlüssel an das Ende ihrer E-Mail-Nachrichten an. Häufig muß der Empfänger dann nur auf diese Adresse doppelklicken, um auf eine Kopie des Schlüssels auf dem Server zugreifen zu können. Es gibt sogar Personen, die ihren PGP-Fingerabdruck zur leichteren Verifizierung auch auf ihren Visitenkarten angeben.

Eigenen öffentlichen Schlüssel in eine E-Mail-Nachricht einfügen

Eine andere praktische Methode zur Weitergabe des eigenen öffentlichen Schlüssels besteht darin, diesen per E-Mail zu versenden.

So fügen Sie Ihren öffentlichen Schlüssel in eine E-Mail-Nachricht ein:

1. Öffnen Sie PGPkeys.
2. Wählen Sie Ihr Schlüsselpaar aus, und wählen Sie den Befehl **Kopieren** aus dem Menü **Bearbeiten**.
3. Öffnen Sie den Editor, den Sie zum Erstellen Ihrer E-Mail-Nachrichten verwenden, setzen Sie den Cursor an die Stelle, an der der Schlüssel eingefügt werden soll, und wählen Sie dann den Befehl **Einfügen** aus dem Menü **Bearbeiten**. In einigen E-Mail-Programmen können Sie den Schlüssel einfach aus PGPkeys in den Textbereich Ihrer E-Mail-Nachricht ziehen.

Wenn Sie jemandem Ihren öffentlichen Schlüssel senden, sollten Sie die E-Mail-Nachricht unterschreiben. Auf diese Weise kann der Empfänger Ihre Unterschrift verifizieren und sicher sein, daß niemand die ursprünglichen Informationen geändert hat. Wenn Ihr Schlüssel noch nicht von einem vertrauenswürdigen Schlüsselverwalter unterschrieben worden ist, können die Empfänger Ihrer Unterschrift nur durch die Verifizierung des Fingerabdrucks auf Ihrem Schlüssel sicher sein, daß die Unterschrift wirklich von Ihnen stammt.

Eigenen öffentlichen Schlüssel in eine Datei exportieren

Eine weitere Möglichkeit zur Weitergabe Ihres öffentlichen Schlüssels besteht darin, ihn in eine Datei zu kopieren und diese Datei dann der Person zur Verfügung zu stellen, mit der Sie kommunizieren möchten.

So exportieren Sie Ihren öffentlichen Schlüssel in eine Datei:

Zum Exportieren oder Speichern Ihres öffentlichen Schlüssels in einer Datei haben Sie drei Möglichkeiten:

- Wählen Sie in PGPkeys das Symbol für Ihr Schlüsselpaar aus, und klicken Sie dann im Menü **Schlüssel** auf **Exportieren**. Geben Sie den Namen der Datei ein, in der Sie den Schlüssel speichern möchten.
- Ziehen Sie das Symbol für Ihr Schlüsselpaar aus PGPkeys in den Ordner, in dem der Schlüssel gespeichert werden soll.
- Wählen Sie in PGPkeys das Symbol für Ihr Schlüsselpaar aus, klicken Sie im Menü **Bearbeiten** auf **Kopieren**, und wählen Sie dann **Einfügen**, um die Schlüsseldaten in ein Textdokument einzufügen.

HINWEIS: Wenn Sie Ihren Schlüssel an Kollegen schicken, die auf PCs arbeiten, geben Sie einen Dateinamen aus maximal 8 Zeichen und den 3 Zeichen der Dateierweiterung ein (beispielsweise MEINSCHL.TXT).

Öffentliche Schlüssel von anderen Benutzern erhalten

Genauso wie Sie Ihre öffentlichen Schlüssel an die Personen verteilen müssen, die verschlüsselte E-Mail-Nachrichten an Sie senden oder Ihre digitale Unterschrift verifizieren möchten, benötigen Sie die öffentlichen Schlüssel von anderen Personen, damit Sie verschlüsselte E-Mail-Nachrichten an diese senden und ihre digitalen Unterschriften verifizieren können.

Es gibt drei Möglichkeiten, den Schlüssel eines anderen Benutzers zu erhalten:

- Sie können sich den Schlüssel von einem Schlüsselserver holen.
- Sie können den öffentlichen Schlüssel Ihrem Schlüsselbund direkt aus einer E-Mail-Nachricht hinzufügen.
- Sie können den öffentlichen Schlüssel aus einer exportierten Datei importieren.

Öffentliche Schlüssel sind einfach nur Textblöcke. Daher ist es ziemlich einfach, sie zu Ihrem Schlüsselbund hinzuzufügen. Importieren Sie sei einfach aus einer Datei, oder kopieren Sie sie aus einer E-Mail-Nachricht, und fügen Sie sie anschließend Ihrem öffentlichen Schlüsselbund hinzu.

Öffentliche Schlüssel von einem Schlüsselserver holen

Wenn der Benutzer, dem Sie eine verschlüsselte Nachricht schicken möchten, ein erfahrener PGP-Benutzer ist, hat er mit hoher Wahrscheinlichkeit eine Kopie seines öffentlichen Schlüssels auf einem Schlüsselserver abgelegt. Dadurch haben Sie jederzeit problemlos Zugang zum aktuellsten Schlüssel, wenn Sie ihm eine Nachricht schicken möchten, und Sie müssen nicht eine Vielzahl von Schlüsseln in Ihrem öffentlichen Schlüsselbund speichern.

Unter Umständen werden Sie vom Administrator Ihres Unternehmens angewiesen, den Schlüsselserver des Unternehmens zu verwenden, auf dem alle in Ihrem Unternehmen häufig verwendete Schlüssel gespeichert sind. In diesem Fall ist Ihre PGP-Software wahrscheinlich bereits darauf konfiguriert, auf den richtigen Server zuzugreifen.

Es stehen mehrere öffentliche Schlüsselserver zur Verfügung (wie z. B. der von Network Associates Inc. unterhaltene Server), auf denen Sie die Schlüssel der meisten PGP-Benutzer finden können. Wenn der Empfänger Ihnen nicht die Web-Adresse genannt hat, unter der sein öffentlicher Schlüssel gespeichert ist, können Sie auf einen beliebigen Schlüsselserver zugreifen und nach dem Namen des Benutzers oder dessen E-Mail-Adresse suchen. Das funktioniert, weil alle Schlüsselserver in regelmäßigen Abständen aktualisiert werden und daher auf allen Servern alle überhaupt auf einem Server gespeicherten Schlüssel gespeichert sind.

So holen Sie sich den öffentlichen Schlüssel eines Benutzers von einem Schlüsselserver:

1. Öffnen Sie PGPkeys.
2. Wählen Sie den Befehl **Suchen** aus dem Menü **Server**, oder klicken Sie in PGPkeys auf **Suchen** ( ).

   Daraufhin wird das **PGPkeys-Suchfenster** angezeigt (siehe Abbildung 3-5).

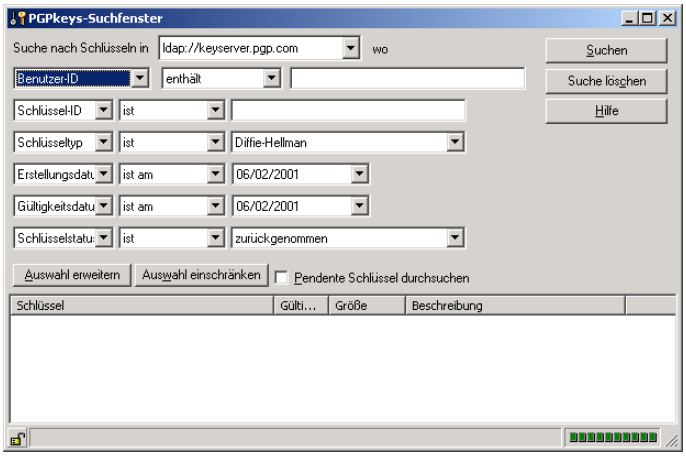


Abbildung 3-5. PGPkeys-Suchfenster (Ansicht *Auswahl erweitern*)

3. Wählen Sie im Menü **Suche nach Schlüsseln in** den zu durchsuchenden Server aus.
4. Geben Sie die Suchkriterien an.

   Sie können nach Schlüsseln auf einem Schlüsselserver suchen, indem Sie Angaben zu mehreren Schlüsseleigenschaften machen:

   Die Umkehrung der meisten dieser Operationen ist ebenfalls möglich. Ihr Kriterium könnte bei einer Suche beispielsweise auch “Benutzer-ID ist nicht Frank” lauten.
5. Geben Sie den zu suchenden Wert an.
6. Klicken Sie auf **Auswahl erweitern**, um der Suche zusätzliche Kriterien hinzuzufügen, wie beispielsweise Schlüssel-IDs mit dem Namen “Susanne”, die am oder vor dem 05.03.1998 erstellt wurden.

7. Starten Sie Ihre Suche durch Klicken auf **Suchen**.

   Eine Statusleiste informiert Sie darüber, wie weit die Suche fortgeschritten ist.

   HINWEIS: Um eine Suche abzubrechen, klicken Sie auf **Suche anhalten**.

   Die Suchergebnisse werden im Fenster angezeigt.

8. Um die gefundenen Schlüssel zu importieren, ziehen Sie sie in das Hauptfenster von PGPkeys.

9. Klicken Sie auf **Suche löschen**, um die Suchkriterien zu entfernen.

Öffentliche Schlüssel aus E-Mail-Nachrichten entnehmen

Die bequemste Art, eine Kopie des öffentlichen Schlüssels einer anderen Person zu erhalten, besteht darin, die betreffende Person zu bitten, den Schlüssel an eine E-Mail-Nachricht anzuhängen. Wenn ein öffentlicher Schlüssel über E-Mail gesendet wird, wird er im Textkörper der Nachricht als Textblock angezeigt.

So entnehmen Sie einen öffentlichen Schlüssel aus einer E-Mail-Nachricht:

- Wenn es für Ihr E-Mail-Programm ein PGP-Plugin gibt, klicken Sie in Ihrem E-Mail-Programm auf , um den öffentlichen Schlüssel des Absenders aus der E-Mail zu extrahieren und Ihrem öffentlichen Schlüsselbund hinzuzufügen.

- Wenn es für Ihr E-Mail-Programm keine Plugins gibt, können Sie den öffentlichen Schlüssel Ihrem Schlüsselbund hinzufügen, indem Sie den Textblock, der den öffentlichen Schlüssel darstellt, kopieren und ihn in PGPkeys einfügen.

Schlüssel und X.509-Zertifikate importieren

Sie können öffentliche PGP-Schlüssel und PKCS-12 X.509-Zertifikate (ein von den meisten Browsern verwendetes digitales Zertifikatsformat) in Ihren öffentlichen Schlüsselbund importieren. Sie können auch X.509-Zertifikate im PEM (Privacy Enhanced Mail)-Format aus Ihrem Browser importieren, indem Sie diese kopieren und in Ihren öffentlichen Schlüsselbund einfügen.

Eine andere Methode, an den öffentlichen Schlüssel einer anderen Person zu gelangen, besteht darin, diese zu bitten, den Schlüssel in einer Datei zu speichern, aus der Sie ihn importieren oder kopieren und in Ihren öffentlichen Schlüsselbund einfügen können.

So importieren Sie einen öffentlichen Schlüssel bzw. ein X.509-Zertifikat aus einer Datei:

Es gibt drei Methoden zum Extrahieren des öffentlichen Schlüssels eines anderen Benutzers und zum Hinzufügen dieses Schlüssel zu Ihrem öffentlichen Schlüsselbund:

- Klicken Sie im Menü **Schlüssel** auf **Importieren**, und gehen Sie dann zu der Datei, in der der öffentliche Schlüssel gespeichert ist.
- Ziehen Sie die Datei, die den öffentlichen Schlüssel enthält, auf das PGPkeys-Hauptfenster.
- Öffnen Sie das Textdokument, in dem der öffentliche Schlüssel gespeichert ist, und markieren Sie den Textblock, der den Schlüssel darstellt. Klicken Sie anschließend im Menü **Bearbeiten** auf **Kopieren**. Wechseln Sie zum PGPkeys-Fenster, und wählen Sie den Befehl **Einfügen** aus dem Menü **Bearbeiten**, um den Schlüssel zu kopieren Der Schlüssel wird dann in PGPkeys als Symbol angezeigt.

Private PKCS-12-X.509-Schlüssel können Sie auch aus Ihrem Browser exportieren und in PGPkeys ziehen oder über den Befehl **Importieren** im Menü **Schlüssel** dem Schlüsselbund hinzufügen.

Echtheit eines Schlüssels verifizieren

Wenn Sie mit einer Person Schlüssel austauschen, läßt sich mitunter nur schwer feststellen, ob der Schlüssel wirklich zu dieser Person gehört.
Die PGP-Software bietet Ihnen eine Reihe von Sicherungsmechanismen, mit denen Sie die Echtheit eines Schlüssels überprüfen und zertifizieren können, daß er einem bestimmten Eigentümer gehört (d. h., die *Echtheit überprüfen* können). Außerdem warnt Sie das PGP-Programm bei dem Versuch, einen Schlüssel zu verwenden, der nicht echt ist. Standardmäßig werden Sie auch gewarnt, bevor Sie einen zweitrangigen, echten Schlüssel verwenden.

Warum sollte man die Echtheit eines Schlüssels verifizieren?

Einer der Hauptangriffspunkte von Verschlüsselungssystemen mit öffentlichen Schlüsseln ist die Fähigkeit von raffinierten Spionen, einen Abfangangriff ("man-in-the-middle attack") durchzuführen, indem sie den öffentlichen Schlüssel eines Benutzers durch ihren eigenen ersetzen. Auf diese Weise kann jede an diese Person gerichtete verschlüsselte E-Mail-Nachricht abgefangen, mit Hilfe eines eigenen Schlüssels entschlüsselt, anschließend wieder mit dem echten Schlüssel der Person verschlüsselt und an diese weitergeleitet werden, als ob niemals etwas geschehen wäre. Diese Handlungen können sogar mit Hilfe spezieller Programme automatisch vorgenommen werden, die zwischen Ihnen und dem Empfänger Ihrer Nachricht stehen und Ihre gesamte Kommunikation entziffern.

In Anbetracht dieses Risikos müssen Sie und diejenigen, mit denen Sie E-Mail-Nachrichten austauschen, sicher sein können, daß die verwendeten Schlüsselkopien wirklich echt sind. Die beste Methode, mit der Sie völlig sicher sein können, daß ein öffentlicher Schlüssel wirklich einer bestimmten Person gehört, besteht darin, den Besitzer darum zu bitten, den Schlüssel auf eine Diskette zu kopieren und Ihnen diese anschließend persönlich auszuhändigen. Meistens werden Sie sich aber nicht in der Nähe derjenigen befinden, von denen Sie eine Diskette benötigen würden. Normalerweise tauschen Sie öffentliche Schlüssel per E-Mail aus oder erhalten sie über einen öffentlichen Schlüsselserver.

Mit digitalen Fingerabdrücken verifizieren

Um festzustellen, ob ein Schlüssel tatsächlich einer bestimmten Person gehört, können Sie den digitalen Fingerabdruck – eine eindeutige Folge von bei der Erstellung des Schlüssels generierten Zahlen oder Worten – überprüfen. Durch einen Vergleich des Originals mit Ihrer Kopie des Fingerabdrucks des öffentlichen Schlüssels einer Person können Sie absolute Gewißheit erlangen, daß es sich tatsächlich um eine gültige Kopie des Schlüssels handelt. Informationen dazu, wie Sie beim Verifizieren anhand eines digitalen Fingerabdrucks vorgehen müssen, finden Sie im Abschnitt "Öffentliche Schlüssel anderer Benutzer verifizieren" auf Seite 76.

Öffentliche Schlüssel überprüfen

Echtheit und Vertrauenswürdigkeit sind zwei komplizierte, dennoch aber äußerst wichtige Begriffe in PGP. Genauere Erörterungen dazu finden Sie in *Einführung in die Kryptographie*. Wenn Sie absolut sicher sind, daß Sie über eine gültige Kopie des öffentlichen Schlüssels eines anderen Benutzers verfügen, können Sie den Schlüssel dieser Person unterschreiben. Wenn Sie den öffentlichen Schlüssel einer anderen Person mit Ihrem privaten Schlüssel unterschreiben, bestätigen Sie, daß Sie sicher sind, daß der Schlüssel tatsächlich dem angegebenen Benutzer gehört. Wenn Sie beispielsweise einen neuen Schlüssel erstellen, wird dieser automatisch mit Ihrer eigenen Unterschrift zertifiziert (bestätigt). Standardmäßig werden Unterschriften, die Sie auf anderen Schlüsseln leisten, nicht exportiert, d.h., sie gelten nur für einen Schlüssel, wenn er sich auf Ihrem Schlüsselbund befindet. Genaue Anweisungen zum Unterschreiben von Schlüsseln finden Sie im Abschnitt “Öffentliche Schlüssel anderer Benutzer unterschreiben” auf Seite 78.

Mit autorisierten Schlüsselverwaltern arbeiten

Oftmals lassen PGP-Benutzer auch ihre öffentlichen Schlüssel durch andere vertrauenswürdige Benutzer unterzeichnen, um ihre Echtheit zusätzlich attestieren zu lassen. Sie können beispielsweise einem Kollegen Ihres Vertrauens eine Kopie Ihres öffentlichen Schlüssels mit der Bitte schicken, den Schlüssel zu zertifizieren und an Sie zurückzuschicken, damit Sie seine Unterschrift einfügen können, wenn Sie den Schlüssel auf einem Server für öffentliche Schlüssel ablegen. Mit PGP müssen die Personen, die eine Kopie Ihres öffentlichen Schlüssels erhalten, nicht selbst die Echtheit des Schlüssels überprüfen, sondern können statt dessen dem Urteil derer vertrauen, die Ihren Schlüssel unterzeichnet haben. PGP gibt Ihnen die Möglichkeit, diesen Grad an Echtheit für jeden öffentlichen Schlüssel festzulegen, den Sie zu Ihrem öffentlichen Schlüsselbund hinzufügen. Außerdem wird der Grad an Echtheit und Vertrauen für jeden Schlüssel angezeigt. Dies bedeutet, daß Sie ziemlich sicher sein können, daß ein Schlüssel vom angegebenen Benutzer stammt, wenn er von einem autorisierten Schlüsselverwalter unterzeichnet wurde. Genauere Informationen zum Unterschreiben von Schlüsseln und zur Authentisierung von Benutzern finden Sie im Abschnitt “Öffentliche Schlüssel anderer Benutzer unterschreiben” auf Seite 78.

Der Sicherheitsbeauftragte Ihres Unternehmens kann als vertrauenswürdiger Schlüsselverwalter agieren, und Sie können dann alle durch den firmenweiten Schlüssel unterzeichneten Schlüssel als gültig betrachten. Wenn Sie für ein großes Unternehmen mit mehreren Niederlassungen arbeiten, haben Sie möglicherweise regionale Schlüsselverwalter, und Ihr Sicherheitsbeauftragter könnte ein höhergestellter Schlüsselverwalter, eine Art autorisierter Schlüsselverwalter der autorisierten Schlüsselverwalter, sein.

Was ist ein autorisierter Schlüsselverwalter?

PGP arbeitet mit sogenannten autorisierten Schlüsselverwaltern, also Personen, deren Schlüssel Sie als vertrauenswürdig ansehen. Bei PGP können Benutzer gegenseitig ihre Schlüssel unterschreiben, um diese zu überprüfen. Wenn Sie einen Schlüssel unterschreiben, bestätigen sie damit dessen Gültigkeit. Sie sind also davon überzeugt, daß der Schlüssel tatsächlich von der entsprechenden Person stammt. Für das Unterschreiben gibt es mehrere Möglichkeiten. Wenn ein autorisierter Schlüsselverwalter einen fremden Schlüssel unterschreibt, werden Sie die Gültigkeit dieses Schlüssels nicht mehr in Frage stellen.

Was ist ein höhergestellter Schlüsselverwalter?

PGP unterstützt außerdem das Konzept sogenannte höhergestellter Schlüsselverwalter – sozusagen eine autorisierte Person für die Vermittlung autorisierter Schlüsselverwalter. Wenn Sie in einem sehr großen Unternehmen arbeiten, wurde möglicherweise ein regionaler Sicherheitsbeauftragter zum Unterschreiben der Benutzerschlüssel bestimmt. Sie könnten in diesem Fall also auf die Gültigkeit dieser Schlüssel vertrauen, da sie bereits durch den regionalen Sicherheitsbeauftragten überprüft wurden. Das Unternehmen kann darüber hinaus aber auch noch einen übergeordneten Sicherheitsbeauftragten haben, der mit den regionalen Sicherheitsbeauftragten zusammenarbeitet, so daß jemand im Büro in Hamburg auch einer Person im Büro in München vertrauen kann. Denn beide haben dann ihre Schlüssel von ihrem jeweiligen regionalen Sicherheitsbeauftragten unterschreiben lassen, deren Schlüssel wiederum von ihrem vorgesetzten Sicherheitsbeauftragten (einem höhergestellten Schlüsselverwalter) unterschrieben wurden. Dies ermöglicht die Einführung einer Vertrauenshierarchie innerhalb des Unternehmens.

Schlüssel verwalten 4

In diesem Kapitel wird beschrieben, wie Sie die in Ihren Schlüsselbunddateien gespeicherten Schlüssel prüfen und verwalten können.

PGP-Schlüsselbunde verwalten

Sowohl die von Ihnen erstellten Schlüssel als auch die Schlüssel, die Sie von anderen erhalten, werden in Schlüsselbunddateien auf der Festplatte oder einer Diskette gespeichert. Ihre privaten Schlüssel werden normalerweise in einer Datei namens secring.skr gespeichert, während die öffentlichen Schlüssel in der Datei pubring.pkr gespeichert werden. Diese Dateien, die sich üblicherweise in Ihrem Ordner **Profile** befinden, können Sie im PGPkeys-Fenster öffnen und dort auch bearbeiten (Abbildung 4-1).

HINWEIS: Da Ihr privater Schlüssel automatisch verschlüsselt wird und Ihre Paßphrase sicher ist, können Ihre Schlüsselbunde gefahrlos auf Ihrem Computer verbleiben. Wenn Sie Ihre Schlüssel jedoch trotzdem nicht im Standardpfad speichern möchten, können Sie einen anderen Dateinamen bzw. einen anderen Ordner festlegen. Informationen dazu finden Sie im Abschnitt “PGP-Optionen festlegen” auf Seite 244.

Gelegentlich kann es erforderlich sein, die mit Ihren Schlüsseln verknüpften Attribute zu überprüfen oder zu ändern. Wenn Sie beispielsweise den öffentlichen Schlüssel eines anderen Benutzers erhalten, kann es sein, daß Sie den Schlüsseltyp (“RSA” oder “Diffie-Hellman/DSS”) bestimmen sowie dessen Fingerabdruck oder seine Gültigkeit anhand der zu dem Schlüssel gehörenden digitalen Unterschriften überprüfen möchten. Darüber hinaus können Sie den öffentlichen Schlüssel eines anderen Benutzers unterschreiben, um die Gültigkeit des Schlüssels zu bestätigen, dem Schlüsseleigentümer ein bestimmtes Maß an Vertrauen aussprechen oder die Paßphrase für Ihren privaten Schlüssel ändern. Vielleicht möchten Sie auch auf einem Schlüsselserver nach dem Schlüssel eines anderen Benutzers suchen. Diese Schlüsselverwaltungsfunktionen werden über PGPkeys ausgeführt.

Das PGPkeys-Fenster

Im PGPkeys-Fenster (siehe Abbildung 4-1) werden Ihre selbst erstellten Schlüssel sowie alle öffentlichen Schlüssel angezeigt, die Sie Ihrem öffentlichen Schlüsselbund hinzugefügt haben. Sämtliche Schlüsselverwaltungsfunktionen werden von diesem Fenster aus ausgeführt.

Das PGPkeys-Fenster öffnen Sie, indem Sie auf **Start—>Programme—>PGP—>PGPkeys** klicken, oder indem Sie auf das PGPtray-Symbol ( ) im Systemfeld der Task-Leiste und dann auf **PGPkeys** klicken.

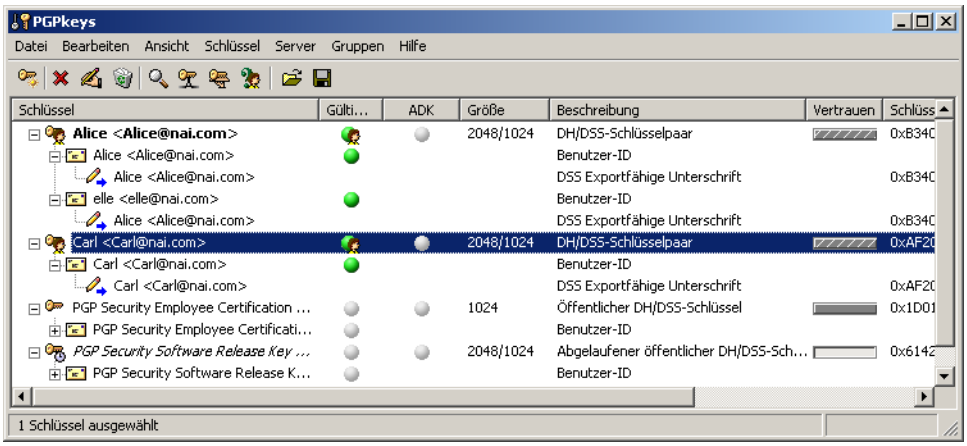


Abbildung 4-1. PGPkeys-Fenster

Definitionen der PGPkeys-Attribute

Einige der mit Schlüsseln verbundenen Attribute können im PGPkeys-Hauptfenster angezeigt werden. Welche Attribute angezeigt werden sollen, können Sie im Menü **Ansicht** festlegen. Für jedes im Menü **Ansicht** ausgewählte Element zeigt PGPkeys im Hauptfenster eine Spalte an. Wenn Sie die Reihenfolge dieser Spalten verändern möchten, klicken Sie auf die Überschrift der zu verschiebenden Spalte, und ziehen Sie sie an die gewünschte Position. Eine Aufstellung der Definitionen der PGPkeys-Attribute finden Sie in Tabelle 4-1 auf Seite 69.

Tabelle 4-1. Überblick über die PGPkeys-Attribute

Attribut	Beschreibung
Schlüssel	Zeigt eine symbolische Darstellung des Schlüssels zusammen mit dem Benutzernamen, der E-Mail-Adresse und einem Foto des Eigentümers sowie die Namen der Unterzeichner des Schlüssels an. Das Symbol mit dem gelben Schlüssel und dem Benutzer steht für Ihr aus Ihrem privaten und Ihrem öffentlichen Schlüssel bestehenden Diffie-Hellman/DSS-Schlüsselpaar. Das Symbol mit dem grauen Schlüssel und dem Benutzer steht für Ihr aus Ihrem privaten und Ihrem öffentlichen Schlüssel bestehenden RSA-Schlüsselpaar. Ein einzelner gelber Schlüssel steht für einen öffentlichen Diffie-Hellman/DSS-Schlüssel. Ein einzelner grauer Schlüssel steht für einen öffentlichen RSA-Schlüssel. Wenn ein Schlüssel oder ein Schlüsselpaar abgeblendet dargestellt wird, können die Schlüssel vorübergehend nicht zum Verschlüsseln und Unterschreiben verwendet werden. Sie können Schlüssel im PGPkeys-Fenster deaktivieren, um zu verhindern, daß selten verwendete Schlüssel stets im PGP-Dialogfeld zur Schlüsselauswahl angezeigt werden. Der mit einem roten X gekennzeichnete Schlüssel steht für einen zurückgenommenen Schlüssel. Benutzer nehmen Ihre Schlüssel zurück, wenn die Schlüssel nicht mehr gültig oder sicher sind. Ein einzelner Schlüssel mit einem Uhrensymbol steht für einen abgelaufenen öffentlichen Schlüssel bzw. ein abgelaufenes Schlüsselpaar. Es können noch weitere Symbole mit einem Schlüssel angezeigt werden, die dann angeben, daß der Schlüssel eine Unterschrift, ein Zertifikat oder eine Foto-Benutzer-ID besitzt. Durch ein Stift- oder ein Füllhaltersymbol werden die Unterschriften der PGP-Benutzer gekennzeichnet, die sich für die Echtheit des Schlüssels verbürgen. - Eine mit einem roten X durchgestrichene Unterschrift gibt an, daß die Unterschrift zurückgenommen wurde. - Eine Unterschrift mit einem abgeblendet dargestellten Stiftsymbol steht für unechte oder ungültige Unterschriften. - Ein blauer Pfeil an einer Unterschrift zeigt an, daß die Unterschrift exportiert werden kann.

Attribut	Beschreibung
Schlüssel	Ein Zertifikatssymbol steht für ein X.509-Zertifikat, einem anerkannten elektronischen Dokument zur Prüfung der Identität und der Eigentümer von öffentlichen Schlüsseln in einem Kommunikationsnetzwerk. Ein Zertifikatssymbol mit einer Uhr steht für ein abgelaufenes X.509-Zertifikat. Ein mit einem roten X versehenes Zertifikatssymbol steht für ein zurückgenommenes X.509-Zertifikat. Dieses Symbol zeigt an, daß eine Foto-Benutzer-ID zum öffentlichen Schlüssel gehört.
Gültigkeit	Gibt den Grad der Gewißheit an, mit der der Schlüssel tatsächlich dem angegebenen Eigentümer gehört. Die Gültigkeit richtet sich nach dem Unterzeichner des Schlüssels und dem Grad Ihres Vertrauens in den/die Unterzeichner, die Gültigkeit eines Schlüssels bestätigen zu können. Die von Ihnen selbst unterschriebenen öffentlichen Schlüssel verfügen über den höchsten Gültigkeitsgrad. Dabei wird davon ausgegangen, daß Sie einen Schlüssel für eine andere Person nur unterschreiben, wenn Sie von der Gültigkeit des Schlüssels absolut überzeugt sind. Die Gültigkeit aller anderen Schlüssel hängt von dem Maß an Vertrauen ab, das Sie den Benutzern aussprechen, die den Schlüssel unterschrieben haben. Wenn mit dem Schlüssel keine Unterschriften verknüpft sind, wird er als nicht gültig angesehen, und bei jeder Verschlüsselung mit dem Schlüssel wird eine entsprechende Meldung angezeigt. Je nachdem, welche Einstellung Sie für **Zweitrangige Gültigkeitsebene anzeigen** in den **Erweiterten Optionen** vorgenommen haben, wird die Gültigkeit durch Kreis- oder Balkensymbole angezeigt (siehe ”Erweiterte Optionen festlegen” weiter hinten in diesem Kapitel). Ist diese Option deaktiviert, wird die Gültigkeit von Schlüsseln wie folgt angezeigt: mit einem grauen Kreis für ungültige und zweitrangige, gültige Schlüssel, wenn unter **Erweiterte Optionen** die Option **Zweitrangige, gültige Schlüssel wie ungültige behandeln** aktiviert ist mit einem grünen Kreis für gültige Schlüssel, die Ihnen nicht gehören mit einem grünen Kreis und einem Benutzer für gültige Schlüssel, die Ihnen gehören Wenn Sie Teil einer Unternehmensumgebung sind, ist es möglich, daß Ihr Sicherheitsbeauftragter die Schlüssel der Benutzer mit dem firmenweiten Unterschriftenschlüssel unterschreibt. Schlüssel mit einer solchen Unterschrift gelten als vollständig echt. Weitere Informationen dazu finden Sie in Kapitel 2, “Kurze Einführung in PGP”.

Attribut	Beschreibung
Größe	In dieser Spalte wird die Bitanzahl angegeben, die bei der Erzeugung des Schlüssels verwendet wurde. Je größer der Schlüssel ist, desto geringer ist normalerweise die Gefahr, daß der Code entschlüsselt wird. Allerdings dauert die Verschlüsselung und Entschlüsselung von Daten bei größeren Schlüsseln etwas länger als bei kleineren Schlüsseln. Wenn Sie einen Diffie-Hellman/DSS-Schlüssel erstellen, steht eine Zahl für den Diffie-Hellman-Anteil und eine andere Zahl für den DSS-Anteil. Der DSS-Anteil wird zum Unterschreiben und der Diffie-Hellman-Anteil für die Verschlüsselung verwendet.
Beschreibung	Beschreibt die Art der in der Spalte **Schlüssel** angezeigten Informationen: Schlüsseltyp, Art der ID bzw. Unterschriftstyp.
Zusätzlicher Entschlüsselungsschlüssel (Additional Decryption Key, ADK)	Zeigt an, ob dem Schlüssel ein Zusätzlicher Entschlüsselungsschlüssel (Additional Decryption Key, ADK) (Additional Decryption Key, ADK) zugeordnet ist.
Schlüssel-ID	Eindeutige Kennummer, die mit dem Schlüssel verknüpft ist. Diese Kennung dient der Unterscheidung zwischen zwei Schlüsseln mit demselben Benutzernamen und derselben E-Mail-Adresse.

Attribut	Beschreibung
Vertrauen	Hier wird das Maß angegeben, in dem Sie dem Schlüsseleigentümer vertrauen, die öffentlichen Schlüssel anderer Personen zu verwalten. Dieses Vertrauen spielt eine Rolle, wenn Sie selbst die Gültigkeit des öffentlichen Schlüssels einer Person nicht verifizieren können und sich daher auf das Urteil anderer Benutzer, die den Schlüssel unterschrieben haben, verlassen müssen. Wenn Sie ein neues Schlüsselpaar erstellen, wird dessen Schlüsseln implizit Vertrauen ausgesprochen. Dies wird durch die gestreiften Vertrauens- oder Gültigkeitsbalken bzw. durch einen grünen Kreis und ein Benutzersymbol angezeigt. Durch einen leeren Balken wird ein unechter Schlüssel oder ein nicht vertrauenswürdiger Benutzer dargestellt. Durch einen halb gefüllten Balken wird ein eingeschränkt gültiger (“zweitrangig echter”) Schlüssel oder gering vertrauenswürdiger Benutzer dargestellt. Durch einen gestreiften Balken wird ein gültiger Schlüssel dargestellt, dessen Eigentümer Sie sind und dem Sie unabhängig von den Unterschriften auf dem Schlüssel vertrauen. Durch einen vollständig ausgefüllten Balken wird ein echter Schlüssel oder ein vertrauenswürdiger Benutzer dargestellt. Wenn Sie einen öffentlichen Schlüssel erhalten, der mit einem Schlüssel eines anderen Benutzers an Ihrem Schlüsselbund unterschrieben wurde, basiert dessen Echtheit auf dem Vertrauen, das Sie dem Unterzeichner dieses Schlüssels ausgesprochen haben. Einen solchen Vertrauensgrad legen Sie im Dialogfeld **Schlüsseleigenschaften** fest. Folgende Optionen stehen Ihnen dabei zur Verfügung: **Nicht Vertrauenswürdig**, **Eingeschränkt** oder **Vertrauenswürdig**.
Ablaufdatum	In dieser Spalte wird das Datum angegeben, an dem der Schlüssel abläuft. Die meisten Schlüssel sind so eingestellt, daß sie nie ihre Gültigkeit verlieren. Es gibt jedoch auch Fälle, in denen ein Benutzer will, daß der Schlüssel nur für eine bestimmte Zeitdauer benutzt wird. Ein einzelner Schlüssel mit einem Uhrensymbol steht für einen abgelaufenen öffentlichen Schlüssel bzw. ein abgelaufenes Schlüsselpaar.
Erstellung	In dieser Spalte wird das Datum der Schlüsselerstellung angegeben. Sie können die Gültigkeit eines Schlüssels zum Teil danach beurteilen, wie lange der Schlüssel schon im Umlauf ist. Wenn ein Schlüssel bereits längere Zeit verwendet wird, ist es unwahrscheinlich, daß jemand versucht, ihn zu ersetzen, da viele Kopien im Umlauf sind. Verlassen Sie sich als Beweis für die Gültigkeit eines Schlüssels jedoch nie allein auf das Erstellungsdatum.

Standardschlüsselpaar am PGP-Schlüsselbund festlegen

Beim Verschlüsseln von Nachrichten oder Dateien gibt Ihnen PGP die Möglichkeit, Ihre Daten zusätzlich mit einem von Ihnen als Standardschlüsselpaar definierten Schlüsselpaar zu verschlüsseln. Dieses Schlüsselpaar ist das Schlüsselpaar, daß PGP standardmäßig verwendet, wenn Sie eine Nachricht oder den öffentlichen Schlüssel eines anderen Benutzers unterschreiben. Ihr Standardschlüsselpaar wird zur Unterscheidung von anderen Schlüsseln in Fettdruck angezeigt. Wenn Sie über mehrere Schlüsselpaare verfügen, empfiehlt es sich, ein Standardschlüsselpaar festzulegen.

So legen Sie Ihr Standardschlüsselpaar fest:

1. Öffnen Sie PGPkeys, und markieren Sie das Schlüsselpaar, das als Standardschlüssel festgelegt werden soll.
2. Wählen Sie im Menü **Schlüssel** die Option **Als Standardschlüssel festlegen**.

   Das ausgewählte Schlüsselpaar wird daraufhin in Fettdruck angezeigt und ist nun Ihr Standardschlüsselpaar.

Schlüssel an Ihrem PGP-Schlüsselbund importieren und exportieren

Die öffentlichen Schlüssel können in der Regel gesendet und empfangen werden, indem der zugrundeliegende Text von einem öffentlichen oder unternehmenseigenen Schlüsselserver kopiert wird. Schlüssel können aber auch ausgetauscht werden, indem sie als separate Textdateien importiert und exportiert werden. So kann ein anderer Benutzer Ihnen eine Diskette mit seinem öffentlichen Schlüssel aushändigen, oder Sie können Ihren öffentlichen Schlüssel über einen FTP-Server zur Verfügung stellen. Genauere Informationen zum Importieren und Exportieren von öffentlichen Schlüsseln finden Sie in “Öffentliche Schlüssel mit anderen Personen austauschen” auf Seite 55.

Schlüssel oder Unterschriften aus Ihrem PGP-Schlüsselbund löschen

Bei Bedarf können Sie Schlüssel oder Unterschriften von Ihrem PGP-Schlüsselbund löschen. Aus einem Schlüsselbund gelöschte Unterschriften oder Schlüssel werden unwiederherstellbar entfernt. Unterschriften und Benutzer-IDs können einem Schlüssel erneut hinzugefügt werden, und ein importierter öffentlicher Schlüssel kann erneut in Ihren Schlüsselbund importiert werden. Ein privater Schlüssel, der nur an diesem Schlüsselbund vorhanden ist, kann jedoch nicht erneut erstellt werden. Außerdem können die Nachrichten, die in den Kopien der öffentlichen Schlüssel verschlüsselt sind, nicht mehr entschlüsselt werden.

HINWEIS: Falls Sie eine mit Ihrem öffentlichen Schlüssel verbundene Unterschrift oder Benutzer-ID auf einem Schlüsselserver löschen möchten, finden Sie die erforderlichen Informationen in “Eigenen Schlüssel auf einem Schlüsselserver aktualisieren” auf Seite 104.

So löschen Sie einen Schlüssel oder eine Unterschrift aus Ihrem PGP-Schlüsselbund:

1. Öffnen Sie PGPkeys, und wählen Sie den Schlüssel oder die Unterschrift aus, den bzw. die Sie löschen möchten.
2. Wählen Sie den Befehl **Löschen** aus dem Menü **Bearbeiten**, oder klicken Sie auf in der PGPkeys-Symbolleiste.

   Das Dialogfeld “Löschen bestätigen” wird angezeigt.
3. Klicken Sie auf **Ja**.

Schlüssel Ihres PGP-Schlüsselbundes deaktivieren und aktivieren

Gelegentlich kann es vorkommen, daß Schlüssel zeitweilig deaktiviert werden sollen. Diese Funktion ist nützlich, wenn Sie einen öffentlichen Schlüssel zum späteren Gebrauch behalten möchten, der Eigentümer jedoch nicht bei jedem Senden einer E-Mail-Nachricht in der Empfängerliste aufgeführt werden soll.

So deaktivieren Sie einen Schlüssel:

1. Öffnen Sie PGPkeys, und wählen Sie den zu deaktivierenden Schlüssel aus.
2. Wählen Sie im Menü **Schlüssel** den Befehl **Deaktivieren**.

   Der Schlüssel wird abgeblendet angezeigt und ist vorübergehend nicht verfügbar.

So aktivieren Sie einen Schlüssel:

1. Öffnen Sie PGPkeys, und wählen Sie den zu aktivierenden Schlüssel aus.
2. Wählen Sie im Menü **Schlüssel** die Option **Aktivieren**.

   Der Schlüssel wird nicht mehr abgeblendet angezeigt und kann wieder verwendet werden.

Schlüsseleigenschaften überprüfen und festlegen

Zusätzlich zu den allgemeinen Attributen, die im PGPkeys-Fenster angezeigt werden, können Sie noch weitere Eigenschaften von Schlüsseln und Teilschlüsseln überprüfen und ändern.

Das Fenster **Schlüsseleigenschaften** enthält die Registerkarten **Allgemein**, **Teilschlüssel**, **Rücknahmeschlüssel** und **ADK**. Auf jeder dieser Registerkarten finden Sie alle notwendigen Informationen zum öffentlichen Schlüssel einer Person. Außerdem können Sie hier die Attribute Ihrer eigenen öffentlichen Schlüssel erstellen, konfigurieren, bearbeiten oder löschen. Genauere Informationen zu den einzelnen Elementen erhalten Sie in den folgenden Abschnitten.

Element:	Siehe:
Registerkarte **Allgemein**	“Allgemeine Schlüsseleigenschaften” auf Seite 75
Registerkarte **Teilschlüssel**	“Teilschlüsseleigenschaften” auf Seite 85
Registerkarte **Rücknahmeschlüssel**	“Eigenschaften zugeordneter Rücknahmeschlüssel” auf Seite 87
Registerkarte **ADK**	“Eigenschaften von zusätzlichen Entschlüsselungsschlüsseln (Additional Decryption Keys, ADK)” auf Seite 90

Allgemeine Schlüsseleigenschaften

Auf der Registerkarte **Allgemein** können Sie mit Hilfe der jeweiligen Fingerabdrücke den öffentlichen Schlüssel anderer Personen überprüfen, Schlüsseln einen Vertrauensgrad zuweisen, die Paßphrase für Ihren eigenen Schlüssel ändern sowie andere Schlüsselattribute anzeigen. Wenn Sie auf die Registerkarte **Allgemein** (Abbildung 4-2 auf Seite 76) für einen bestimmten Schlüssel zugreifen möchten, wählen Sie den gewünschten Schlüssel aus, und wählen Sie dann den Befehl **Schlüsseleigenschaften** aus dem Menü **Schlüssel**.

Abbildung 4-2. Dialogfeld “Schlüsseleigenschaften” (Registerkarte “Allgemein”)

Öffentliche Schlüssel anderer Benutzer verifizieren

In der Vergangenheit war es schwierig, mit Sicherheit festzustellen, ob ein Schlüssel einer bestimmten Person gehörte, wenn diese Person Ihnen ihren Schlüssel nicht persönlich auf einer Diskette übergab. Diese Art des Austausches von Schlüsseln ist in der Regel etwas unpraktisch, insbesondere für die Benutzer, deren Wohn- bzw. Arbeitsorte weit auseinanderliegen.

Es gibt verschiedene Möglichkeiten zur Überprüfung des Fingerabdrucks eines Schlüssels. Die sicherste Art ist ein direkter Anruf bei der entsprechenden Person, damit der Fingerabdruck telefonisch durchgegeben werden kann. Sofern diese Person nicht das Ziel eines Angriffs ist, ist es sehr unwahrscheinlich, daß jemand diesen zufälligen Anruf abfangen und sich für die Person ausgeben könnte, die Sie anrufen möchten. Sie können außerdem den Fingerabdruck Ihrer Kopie des öffentlichen Schlüssels einer Person mit dem Fingerabdruck des Originalschlüssels dieser Person vergleichen, der sich auf einem öffentlichen Schlüsselserver befindet.

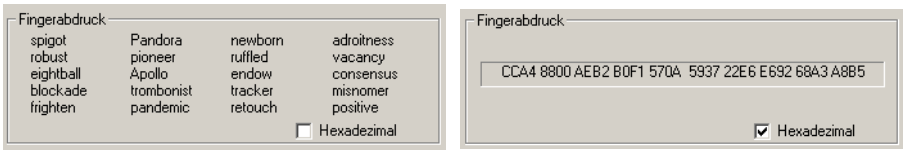
Für die Anzeige des Fingerabdrucks gibt es zwei Möglichkeiten: entweder als eindeutige Liste von Wörtern oder im hexadezimalen Format.

So überprüfen Sie einen öffentlichen Schlüssel anhand seines digitalen Fingerabdrucks:

1. Öffnen Sie PGPkeys, und wählen Sie den zu überprüfenden öffentlichen Schlüssel aus.
2. Wählen Sie im Menü **Schlüssel** den Befehl **Schlüsseleigenschaften**, oder klicken Sie auf .

   Das Dialogfeld “Schlüsseleigenschaften” wird geöffnet (siehe Abbildung 4-2).
3. Vergleichen Sie die im Textfeld **Fingerabdruck** angezeigte Folge von Wörtern oder Zeichen mit dem Originalabdruck.

   Standardmäßig wird im Textfeld **Fingerabdruck** eine Wortliste angezeigt (siehe Abbildung 4-3). Sie können jedoch die Option **Hexadezimal** aktivieren, um den Fingerabdruck in Form von 20 Hexadezimalzeichen anzuzeigen (siehe Abbildung 4-3).



Wortliste *Hexadezimales Format*

Abbildung 4-3. Textfeld “Fingerabdruck”

Die im Textfeld **Fingerabdruck** enthaltene Wortliste besteht aus speziellen, von PGP verwendeten Authentisierungswörtern, die aufgrund ihrer phonetischen Deutlichkeit und ihres leichten Verständnisses ohne Verwechslungsgefahr mit phonetisch ähnlichen Wörtern sorgfältig ausgewählt wurden.

Die Wortliste dient einem ähnlichen Zweck wie das militärische Alphabet, mit dem Piloten Informationen auch über qualitativ schlechte Funkverbindungen deutlich übertragen können. Weitere Informationen zum Wort-Hash-Verfahren und zum Anzeigen als Wortliste finden Sie in Anhang E, “Liste biometrischer Worte”.

Öffentliche Schlüssel anderer Benutzer unterschreiben

Wenn Sie ein Schlüsselpaar erstellen, werden die Schlüssel automatisch von sich selbst unterschrieben. Auf ähnliche Weise können Sie, wenn Sie sicher sind, daß ein Schlüssel zu einer bestimmten Person gehört, den öffentlichen Schlüssel dieser Person unterschreiben. Damit geben Sie an, daß Sie sicher sind, daß es sich um einen gültigen Schlüssel handelt. Wenn Sie den öffentlichen Schlüssel eines anderen Benutzers unterschreiben, wird diesem Schlüssel ein Unterschriftensymbol mit Ihrem Benutzernamen angehängt.

So unterschreiben Sie öffentliche Schlüssel anderer Benutzer:

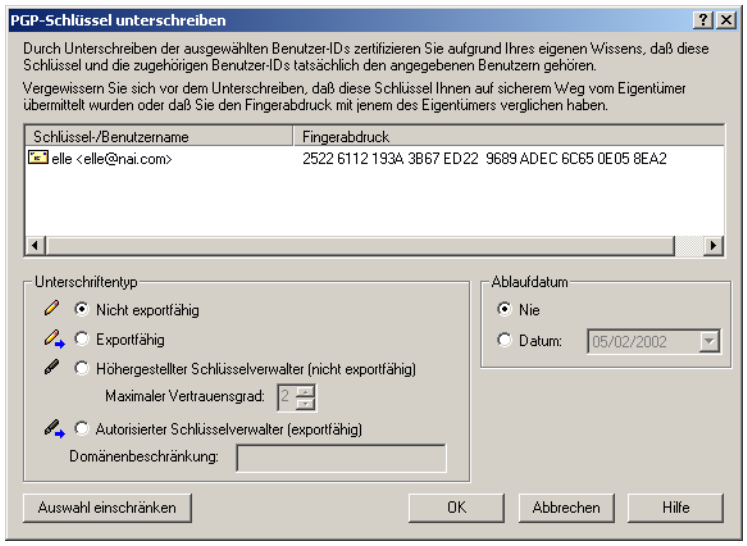
1. Öffnen Sie PGPkeys, und wählen Sie den zu unterschreibenden öffentlichen Schlüssel aus.
2. Wählen Sie im Menü **Schlüssel** die Option **Unterschreiben**, oder klicken Sie auf .

   Das Dialogfeld “PGP-Schlüssel unterschreiben” wird angezeigt, in dessen Textfeld der öffentliche Schlüssel und der Fingerabdruck angezeigt werden.
3. Aktivieren Sie die Option **Exportieren der Unterschrift zulassen**, damit Ihre Unterschrift zusammen mit diesem Schlüssel exportiert werden kann.

   Eine exportierbare Unterschrift kann an Server gesendet werden und wird stets mit dem Schlüssel weitergegeben, wenn dieser beispielsweise durch Ziehen in eine E-Mail-Nachricht exportiert wird. Mit dieser Option können Sie auf einfache Art angeben, daß Ihre Unterschrift exportiert werden soll.

   oder

   Klicken Sie auf die Schaltfläche **Auswahl erweitern** (Abbildung 4-4), wenn Sie weitere Optionen, wie den Unterschriftstyp und die Gültigkeitsdauer der Unterschrift, festlegen möchten.



Weitere Unterschrifts-optionen

Abbildung 4-4. Dialogfeld “PGP-Schlüssel unterschreiben” (erweiterte Auswahl)

Wählen Sie den Unterschriftstyp, mit dem der öffentliche Schlüssel unterzeichnet werden soll. Folgende Optionen stehen zur Verfügung:

- **Nicht exportfähig:** Verwenden Sie diese Unterschrift, wenn Sie überzeugt sind, daß der Schlüssel echt ist, wenn Sie aber nicht möchten, daß sich andere auf Ihre Einschätzung verlassen. Dieser Unterschriftstyp kann nicht mit dem dazugehörigen Schlüssel an einen Schlüsselserver gesendet oder auf andere Weise exportiert werden.
- **Exportfähig:** Verwenden Sie exportfähige Unterschriften dann, wenn Ihre Unterschrift mit dem Schlüssel an den Schlüsselserver gesendet werden soll und sich andere Benutzer auf Ihre Unterschrift verlassen und infolgedessen den von Ihnen unterschriebenen Schlüsseln vertrauen sollen. Dieses Vorgehen entspricht dem Aktivieren der Option **Export der Unterschrift zulassen** im Menü **PGP-Schlüssel unterschreiben**.

- **Höhergestellter Schlüsselverwalter (nicht exportfähig):** Bestätigt, daß dieser Schlüssel sowie alle mit diesem Schlüssel mit einer Bestätigung als autorisierter Schlüsselverwalter unterschriebenen Schlüssel von Ihnen als vollständig autorisierter Schlüsselverwalter akzeptiert wurden. Dieser Unterschriftstyp kann nicht exportiert werden.

  Mit der Option **Maximaler Vertrauensgrad** wird angegeben, bis zu welcher Ebene hinunter Sie autorisierte Schlüsselverwalter ineinander einbetten können. Wenn Sie diesen Grad auf 1 festlegen, ist nur eine Ebene von Schlüsselverwaltern unter der Ebene des höhergestellten Schlüsselverwalters zulässig.

- **Autorisierter Schlüsselverwalter (exportfähig):** Verwenden Sie diese Unterschrift, um die Gültigkeit eines Schlüssels zu zertifizieren und anzugeben, daß dem Schlüsseleigentümer vollständiges Vertrauen entgegengebracht werden sollte, wenn er sich für andere Schlüssel verbürgt. Dieser Unterschriftstyp kann exportiert werden. Sie können die Befugnisse des autorisierten Schlüsselverwalters auf eine bestimmte E-Mail-Domäne einschränken.

4. Wenn Sie die Befugnisse eines autorisierten Schlüsselverwalters zur Überprüfung von Schlüsseln auf eine Einzeldomäne beschränken möchten, geben Sie in das Textfeld **Domänenbeschränkung** den Domänennamen ein.

5. Wenn Sie dieser Unterschrift ein Gültigkeitsdatum zuordnen möchten, geben Sie in das Textfeld **Datum** das Datum ein, an dem diese Unterschrift ablaufen soll. Andernfalls ist die Unterschrift uneingeschränkt gültig.

6. Klicken Sie auf **OK**.

   Das Dialogfeld “Paßphrase” wird angezeigt.

7. Geben Sie Ihre Paßphrase ein, und klicken Sie auf **OK**.

   Dem gerade von Ihnen unterschriebenen Schlüssel wird ein mit Ihrem Benutzernamen verknüpftes Symbol hinzugefügt.

Vertrauen für Schlüsselüberprüfungen aussprechen

Neben der Zertifizierung, daß ein Schlüssel zu einer bestimmten Person gehört, können Sie den Schlüsseleigentümern auch ein bestimmtes Maß an Vertrauen aussprechen. Sie drücken damit aus, inwiefern Sie diesen Personen vertrauen, die Gültigkeit von Schlüsseln anderer Personen als Schlüsselverwalter zu gewährleisten. Wenn Sie also einen Schlüssel erhalten, der von einer Person unterschrieben wurde, der Sie Vertrauen ausgesprochen haben, wird dieser Schlüssel als echt betrachtet werden, obwohl Sie den Schlüssel nicht selbst überprüft haben.

So sprechen Sie Ihr Vertrauen für einen Schlüssel aus:

1. Öffnen Sie PGPkeys, und wählen Sie den Schlüssel aus, dessen Vertrauensgrad Sie ändern möchten.

   HINWEIS: Bevor Sie den Vertrauensgrad für einen Schlüssel ändern können, müssen Sie ihn unterschreiben. Wenn Sie den Schlüssel noch nicht unterschrieben haben, finden Sie Anweisungen dazu im Abschnitt “Öffentliche Schlüssel überprüfen” auf Seite 64.

2. Wählen Sie im Menü **Schlüssel** den Befehl **Schlüsseleigenschaften**, oder klicken Sie auf , um das Dialogfeld “Schlüsseleigenschaften” zu öffnen (siehe Abbildung 4-2).

3. Stellen Sie den gewünschten Vertrauensgrad für das Schlüsselpaar mit dem Schieberegler ein.

Abbildung 4-5. Dialogfeld zur Einstellung des gewünschten Vertrauensgrades

4. Schließen Sie das Dialogfeld, damit die neue Einstellung übernommen wird.

Eigene Paßphrase ändern

Es empfiehlt sich, Ihre Paßphrase in regelmäßigen Abständen, beispielsweise alle drei Monate, zu ändern. Noch wichtiger ist jedoch, daß Sie Ihre Paßphrase sofort ändern, wenn Sie das Gefühl haben, daß sie unsicher geworden ist, beispielsweise, wenn Sie bei der Eingabe beobachtet wurden.

So ändern Sie Ihre Paßphrase:

1. Öffnen Sie PGPkeys, und wählen Sie den Schlüssel aus, dessen Paßphrase Sie ändern möchten.

   Wählen Sie im Menü **Schlüssel** die Option **Schlüsseleigenschaften**, oder klicken Sie auf .

   Das Dialogfeld “Schlüsseleigenschaften” wird geöffnet (siehe Abbildung 4-2).

2. Klicken Sie auf der Registerkarte **Allgemein** auf **Paßphrase ändern**.

   Das Dialogfeld “Paßphrase” wird angezeigt.

HINWEIS: Wenn Sie die Paßphrase für einen geteilten Schlüssel ändern möchten, müssen Sie zuerst die Schlüsselteile wieder zusammensetzen. Klicken Sie auf **Zusammensetzen**, um die Schlüsselteile zusammenzuführen. Informationen dazu, wie Sie dabei vorgehen müssen, finden Sie im Abschnitt “Dateien mit einem geteilten Schlüssel unterschreiben und entschlüsseln” auf Seite 132.

---

3. Geben Sie Ihre aktuelle Paßphrase in dem dafür vorgesehenen Feld ein, und klicken Sie dann auf **OK**.

   Das Dialogfeld “Eingabe und Bestätigung der Paßphrase” wird angezeigt.

4. Geben Sie Ihre neue Paßphrase in das erste Textfeld ein. Drücken Sie die Tabulatortaste, um den Cursor in das nächste Textfeld zu setzen. Bestätigen Sie Ihre Eingabe, indem Sie Ihre neue Paßphrase nochmals eingeben.

5. Klicken Sie auf **OK**.

WARNUNG: Wenn Sie Ihre Paßphrase ändern, weil Sie glauben, daß sie unsicher geworden ist, sollten Sie alle Sicherungskopien Ihrer Schlüsselbunde löschen sowie Ihren freien Speicherplatz bereinigen.

Neue Benutzernamen und Adressen einem Schlüsselpaar hinzufügen

Möglicherweise möchten Sie das gleiche Schlüsselpaar für mehrere Benutzernamen bzw. E-Mail-Adressen verwenden. Nach dem Erstellen eines neuen Schlüsselpaares können Sie dem Schlüssel weitere Namen und Adressen hinzufügen. Sie können neue Benutzernamen oder E-Mail-Adressen aber nur dann hinzufügen, wenn Sie sowohl den privaten als auch die entsprechenden öffentlichen Schlüssel haben.

So fügen Sie Schlüsseln neue Benutzernamen und Adressen hinzu:

1. Öffnen Sie PGPkeys, und wählen Sie das Schlüsselpaar aus, dem Sie einen neuen Benutzernamen oder eine neue Adresse hinzufügen möchten.

2. Wählen Sie den Befehl **Hinzufügen/Name** aus dem Menü **Schlüssel**.

   Das Dialogfeld “Neuer PGP-Benutzername” wird angezeigt.

3. Geben Sie den neuen Namen und die neue E-Mail-Adresse in die betreffenden Felder ein, und klicken Sie auf **OK**.

   Das Dialogfeld “PGP-Paßphrase eingeben” wird angezeigt.

4. Geben Sie Ihre Paßphrase ein, und klicken Sie auf **OK**.

   Der neue Name wird am Ende der zum Schlüssel gehörenden Benutzernamenliste hinzugefügt. Wenn Sie den neuen Benutzernamen und die neue Benutzeradresse als primäre Kennung für Ihren Schlüssel festlegen möchten, markieren Sie den Namen und die Adresse, und wählen Sie im Menü **Schlüssel** den Befehl **Als Primärname einstellen**.

WICHTIG: Wenn Sie an Ihrem Schlüsselpaar Änderungen vornehmen bzw. diesem Informationen hinzufügen, müssen Sie stets das Schlüsselpaar auf dem Schlüsselserver aktualisieren, so daß allen die neueste Version Ihres Schlüssels zur Verfügung steht. Anweisungen dazu finden Sie im Abschnitt “Eigenen Schlüssel auf einem Schlüsselserver aktualisieren” auf Seite 104.

Foto-IDs zu Schlüsseln hinzufügen

In Ihre PGP-Schlüssel können Sie eine Foto-Benutzerkennung aufnehmen.

HINWEIS: Diese Funktion steht nur für Diffie-Hellman / DSS- und RSA-Schlüssel zur Verfügung. Von RSA Legacy-Schlüsseln wird die Foto-ID-Funktion nicht unterstützt.

WICHTIG: Obwohl Sie zum Verifizieren die Foto-ID anzeigen können, die Sie mit einem Schlüssel erhalten, sollten Sie stets die digitalen Fingerabdrücke überprüfen und vergleichen. Weitere Informationen zur Authentisierung finden Sie im Abschnitt “Öffentliche Schlüssel anderer Benutzer verifizieren” auf Seite 76.

So fügen Sie Ihr Foto Ihrem Schlüssel hinzu:

1. Öffnen Sie PGPkeys, wählen Sie Ihr Schlüsselpaar aus, und klicken Sie dann im Menü **Schlüssel** auf den Befehl **Hinzufügen/Foto**.

   Das Dialogfeld “Foto hinzufügen” wird angezeigt.

2. Ziehen Sie Ihr Foto auf das Dialogfeld “Foto hinzufügen”, fügen Sie es ein oder gehen Sie durch Klicken auf **Datei auswählen** zu dessen Speicherort.

HINWEIS: Das Foto kann sich entweder in der Zwischenablage befinden, oder es kann eine JPG- oder BMP-Datei sein. Zur Erzielung einer optimalen Bildqualität sollten Sie das Bild vor dem Einfügen in das Dialogfeld “Foto hinzufügen” auf 120 x 144 Pixel beschneiden. Andernfalls übernimmt PGP die Skalierung des Bildes für Sie.

3. Klicken Sie auf **OK**.

   Das Dialogfeld “Paßphrase” wird angezeigt.

4. Geben Sie in dem dafür vorgesehenen Feld Ihre Paßphrase ein, und klicken Sie dann auf **OK**.

   Ihre Foto-Benutzer-ID wird Ihrem öffentlichen Schlüssel hinzugefügt und im PGPkeys-Fenster aufgeführt.

WICHTIG: Wenn Sie an Ihrem Schlüsselpaar Änderungen vornehmen bzw. diesem Informationen hinzufügen, müssen Sie stets das Schlüsselpaar auf dem Schlüsselserver aktualisieren, so daß allen die neueste Version Ihres Schlüssels zur Verfügung steht. Anweisungen dazu finden Sie im Abschnitt “Eigenen Schlüssel auf einem Schlüsselserver aktualisieren” auf Seite 104.

So tauschen Sie Ihre Foto-ID aus:

1. Öffnen Sie PGPkeys, und wählen Sie das unter Ihrem Schlüssel aufgeführte Foto aus.

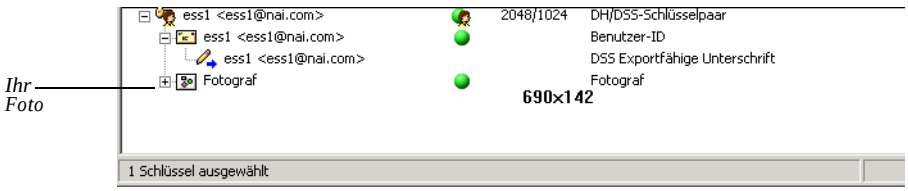


Abbildung 4-6. PGPkeys (Beispiel: Foto-Benutzer-ID)

2. Wählen Sie im Menü **Bearbeiten** den Befehl **Löschen**.

3. Fügen Sie Ihre neue Foto-ID unter Einhaltung der Anweisungen im Abschnitt “So fügen Sie Ihr Foto Ihrem Schlüssel hinzu:” auf Seite 83 hinzu.

Teilschlüsseleigenschaften

Wenn Sie sich die Teilschlüsseleigenschaften für einen bestimmten Schlüssel anzeigen lassen möchten, markieren Sie den gewünschten Schlüssel, und wählen Sie anschließend im Menü **Schlüssel** den Befehl **Schlüsseleigenschaften**. Das Dialogfeld "Schlüsseleigenschaften" wird angezeigt. Klicken Sie auf die Registerkarte **Teilschlüssel**, um sie zu öffnen (siehe Abbildung 4-7).

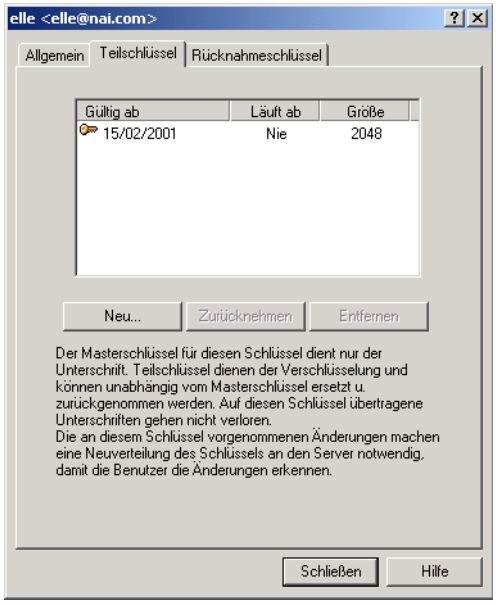


Abbildung 4-7. Dialogfeld "Schlüsseleigenschaften" (Registerkarte "Teilschlüssel")

Neue Teilschlüssel erstellen

Jeder Diffie-Hellman- / DSS-Schlüssel und jeder RSA-Schlüssel besteht aus zwei Schlüsseln: einem Unterschriftenschlüssel und einem Verschlüsselungsteilschlüssel. PGP bietet seit Version 6.0 die Möglichkeit, neue Verschlüsselungsschlüssel zu erstellen und wieder zurückzunehmen, ohne Ihren Haupt-Unterzeichnerschlüssel und die auf ihm gesammelten Unterschriften aufgeben zu müssen. Diese Funktion wird meist zum Erstellen mehrerer Teilschlüssel verwendet, die für die zeitlich versetzte Verwendung während der Lebensdauer des Schlüssels vorgesehen sind. Wenn Sie beispielsweise einen Schlüssel erstellen, der nach drei Jahren ungültig wird, erstellen Sie möglicherweise auch drei Teilschlüssel. Jeder dieser Teilschlüssel wird für ein Jahr der Lebensdauer des Schlüssels verwendet. Dies stellt eine nützliche Sicherheitsmaßnahme dar und automatisiert das regelmäßige Umschalten auf einen neuen Verschlüsselungsschlüssel, ohne daß erneut ein neuer öffentlicher Schlüssel erstellt und verteilt werden muß.

HINWEIS: Diese Funktion steht nur für Diffie-Hellman / DSS- und RSA-Schlüssel zur Verfügung. Bei RSA Legacy-Schlüsseln werden keine Teilschlüssel unterstützt.

So erstellen Sie neue Teilschlüssel:

1. Öffnen Sie PGPkeys, wählen Sie Ihr Schlüsselpaar aus, und klicken Sie dann im Menü **Schlüssel** auf den Befehl **Schlüsseleigenschaften**, oder klicken Sie auf .

   Das Dialogfeld “Schlüsseleigenschaften” wird angezeigt.

2. Klicken Sie auf die Registerkarte **Teilschlüssel**, um sie zu öffnen (siehe Abbildung 4-8 auf Seite 86).

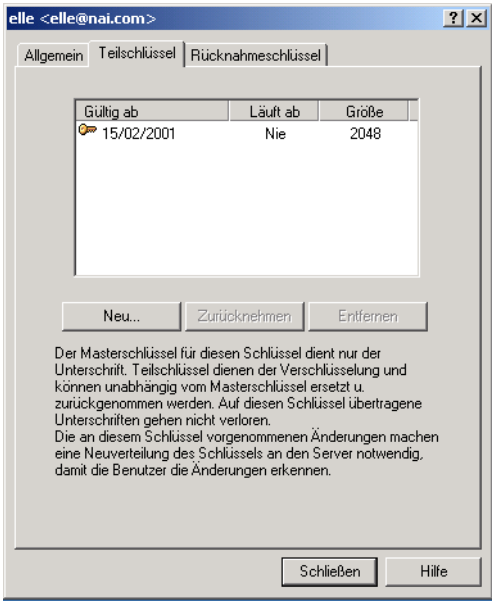


Abbildung 4-8. PGP-Schlüsseleigenschaften (Dialogfeld “Teilschlüssel”)

3. Klicken Sie auf **Neu**, um einen neuen Teilschlüssel zu erstellen.

   Das Dialogfeld “Neuer Teilschlüssel” wird geöffnet.

4. Geben Sie eine Schlüsselgröße zwischen 1024 und 3072 Bit ein. Sie können auch eine benutzerdefinierte Schlüsselgröße zwischen 1024 und 4096 Bit eingeben.

5. Geben Sie das Anfangsdatum an, an dem der Teilschlüssel aktiviert werden soll.
6. Geben Sie das Datum an, an dem der Teilschlüssel ungültig werden soll. Verwenden Sie entweder die Standardeinstellung **Nie**, wenn er niemals ungültig werden soll, oder geben Sie ein bestimmtes Datum ein, nach dem der Teilschlüssel seine Gültigkeit verlieren soll.

HINWEIS: Wenn Sie mehr als einen Teilschlüssel an Ihrem Schlüsselbund verwalten, sollten Sie darauf achten, daß sich die Anfangs- und Ablaufdaten Ihrer Teilschlüssel nicht überschneiden, um Verwirrung zu vermeiden.

---

7. Klicken Sie auf **OK**.

   Das Dialogfeld “Paßphrase” wird angezeigt.
8. Geben Sie Ihre Paßphrase ein, und klicken Sie auf **OK**.

   Der neue Teilschlüssel wird im Teilschlüsselfenster aufgeführt.

WICHTIG: Wenn Sie an Ihrem Schlüsselpaar Änderungen vornehmen bzw. diesem Informationen hinzufügen, müssen Sie stets das Schlüsselpaar auf dem Schlüsselserver aktualisieren, so daß allen die neueste Version Ihres Schlüssels zur Verfügung steht. Anweisungen dazu finden Sie im Abschnitt “Eigenen Schlüssel auf einem Schlüsselserver aktualisieren” auf Seite 104.

Eigenschaften zugeordneter Rücknahmeschlüssel

Um auf die Registerkarte **Rücknahmeschlüssel** für einen bestimmten Schlüssel zuzugreifen, markieren Sie den gewünschten Schlüssel, und wählen Sie anschließend im Menü **Schlüssel** den Befehl **Schlüsseleigenschaften**.
Das Dialogfeld “Schlüsseleigenschaften” wird geöffnet (siehe Abbildung 4-2 auf Seite 76). Klicken Sie auf die Registerkarte **Rücknahmeschlüssel**. Die Registerkarte **Rücknahmeschlüssel** wird angezeigt (siehe Abbildung 4-7).
(Hinweis: Wenn es für den markierten Schlüssel keine zugeordneten Rücknahmeschlüssel gibt, wird die Registerkarte **Rücknahmeschlüssel** auch nicht angezeigt.)

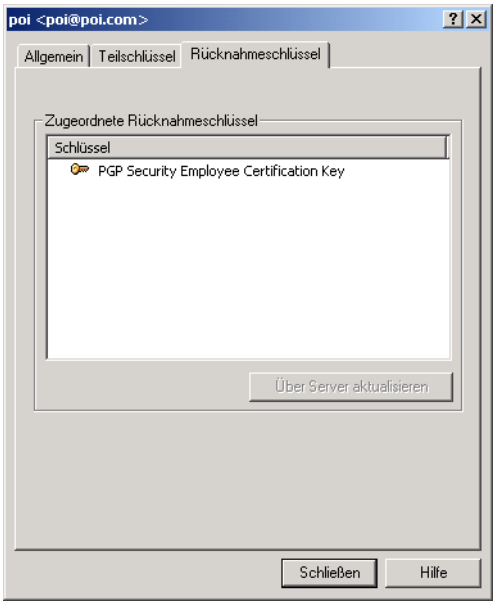


Abbildung 4-9. Dialogfeld “Schlüsseleigenschaften” (Registerkarte “Rücknahmeschlüssel”)

Auf der Registerkarte **Rücknahmeschlüssel** sind alle die Schlüssel aufgeführt, mit denen Sie Ihren PGP-Schlüssel zurücknehmen können. Mit Hilfe der Schaltfläche **Über Server aktualisieren** können Sie hier außerdem auf bequeme Weise Rücknahmeschlüssel aktualisieren.

Wenn sich der zum jeweiligen Schlüssel gehörende Rücknahmeschlüssel nicht an Ihrem Schlüsselbund befindet, wird statt der Benutzer-ID *Unbekannter Schlüssel*, gefolgt von der Schlüssel-ID des Schlüssels angezeigt. Markieren Sie die Schlüssel-ID, und klicken Sie auf die Schaltfläche **Über Server aktualisieren**, um auf dem Schlüsselserver nach dem Schlüssel zu suchen.

Zugeordneten Rücknahmeschlüssel festlegen

Es kann passieren, daß Ihre Paßphrase verloren geht oder Sie einmal Ihren privaten Schlüssel verlieren (wenn z. B. Ihr Notebook gestohlen wird oder Ihre Festplatte kaputt geht). Sofern Ihnen die Möglichkeit der Schlüsselrekonstruktion nicht zur Verfügung steht, sind Sie weder in der Lage, Ihren Schlüssel wieder zu verwenden, noch können Sie ihn zurücknehmen und damit andere Personen daran hindern, weiterhin mit diesem Schlüssel zu verschlüsseln. Um sich gegen diesen Fall abzusichern, können Sie für die Zurücknahme Ihres Schlüssels einen anderen Schlüssel zum Rücknahmeschlüssel machen. Der Halter dieses anderen Schlüssels kann dann, so wie Sie selbst zuvor, Ihren Schlüssel zurücknehmen.

HINWEIS: Damit ein Schlüssel für andere Benutzer als zurückgenommen erkennbar ist, muß sich sowohl der zurückgenommene Schlüssel als auch der zugeordnete Rücknahmeschlüssel am Schlüsselbund der betreffenden Person befinden. Folglich ist die Funktion des zugeordneten Rücknahmeschlüssels am effektivsten in Unternehmensumgebungen, wo sich der zugeordnete Rücknahmeschlüssel des Unternehmens an den Schlüsselbunden sämtlicher Benutzer befindet. Wenn jemand auf seinem Schlüsselbund nicht über den Rücknahmeschlüssel verfügt, kann die betreffende Person nicht erkennen, welche Schlüssel zurückgenommen wurden. Unter Umständen verwendet der- oder diejenige dann bereits zurückgenommene Schlüssel weiter zum Verschlüsseln.

HINWEIS: Diese Funktion steht nur für Diffie-Hellman / DSS- und RSA-Schlüssel zur Verfügung. Bei RSA Legacy-Schlüsseln wird die Schlüsselrücknahme nicht unterstützt.

So fügen Sie einen zugeordneten Rücknahmeschlüssel Ihrem öffentlichen Schlüssel hinzu:

1. Öffnen Sie PGPkeys, und wählen Sie das Schlüsselpaar aus, dem Sie einen Rücknahmeschlüssel hinzufügen möchten.
2. Wählen Sie im Menü **Schlüssel** den Befehl **Hinzufügen/Rücknahmeschlüssel**.

   Das angezeigte Dialogfeld enthält eine Liste mit Schlüsseln.
3. Wählen Sie in der Benutzer-ID-Liste den oder die Schlüssel, die Sie als zugeordnete Rücknahmeschlüssel verwenden möchten.
4. Klicken Sie auf **OK**.

   Ein Dialogfeld zur Bestätigung des Vorgangs wird angezeigt.
5. Klicken Sie auf **OK**, um fortzufahren.

   Das Dialogfeld “Paßphrase” wird angezeigt.
6. Geben Sie Ihre Paßphrase ein, und klicken Sie auf **OK**.
7. Die gewählten Schlüssel sind jetzt autorisierte Rücknahmeschlüssel. Zur Optimierung der Schlüsselverwaltung sollten Sie eine aktuelle Kopie Ihres Schlüssels an die Rücknahmeschlüssel verteilen oder den Schlüssel auf den Server laden. Anweisungen dazu finden Sie im Abschnitt “Eigenen öffentlichen Schlüssel weitergeben” auf Seite 55.

Schlüssel zurücknehmen

Sollte der Fall eintreten, daß Ihr persönliches Schlüsselpaar nicht mehr sicher ist, können Sie mit Hilfe einer Zurücknahme veranlassen, daß Ihr öffentlicher Schlüssel nicht mehr benutzt wird. Ein zurückgenommener Schlüssel läßt sich am besten in Umlauf bringen, indem er auf einem öffentlichen Schlüsselserver abgelegt wird.

So nehmen Sie einen Schlüssel zurück:

1. Öffnen Sie PGPkeys, und wählen Sie das Schlüsselpaar aus, das Sie zurücknehmen möchten.
2. Wählen Sie den Befehl **Zurücknehmen** aus dem Menü **Schlüssel**.

   Das Dialogfeld “Bestätigung der Zurücknahme” wird angezeigt.
3. Klicken Sie auf **OK**, um die Zurücknahme des ausgewählten Schlüssels zu bestätigen.

   Das Dialogfeld “PGP-Paßphrase eingeben” wird angezeigt.
4. Geben Sie Ihre Paßphrase ein, und klicken Sie auf **OK**.

   Wenn Sie einen Schlüssel zurücknehmen, wird er mit einem roten X durchgestrichen, um anzuzeigen, daß er nicht mehr gültig ist.
5. Senden Sie den zurückgenommenen Schlüssel an den Server, so daß alle anderen PGP-Benutzer wissen, daß sie Ihren alten Schlüssel nicht mehr verwenden sollen.

Eigenschaften von zusätzlichen Entschlüsselungsschlüsseln (Additional Decryption Keys, ADK)

Um auf die Registerkarte **ADK** für einen bestimmten Schlüssel zuzugreifen, markieren Sie den gewünschten Schlüssel, und wählen Sie anschließend im Menü **Schlüssel** den Befehl **Schlüsseleigenschaften**. Das Dialogfeld “Schlüsseleigenschaften” wird geöffnet (siehe Abbildung 4-2 auf Seite 76). Klicken Sie auf den Reiter der Registerkarte **ADK**. Die Registerkarte **ADK** wird angezeigt. (Hinweis: Wenn es für den markierten Schlüssel keinen zusätzlichen Entschlüsselungsschlüssel gibt, wird die Registerkarte **ADK** nicht angezeigt.)

Auf der Registerkarte **ADK** werden alle zusätzlichen Entschlüsselungsschlüssel (ADKs) für den ausgewählten Schlüssel aufgeführt. ADKs sind Schlüssel, mit denen die Sicherheitsbeauftragten eines Unternehmens Nachrichten entschlüsseln können, die an oder von Personen innerhalb Ihres Unternehmens gesendet wurden. Es gibt folgende Schlüsseltypen: Zusätzliche Entschlüsselungsschlüssel für eingehende Nachrichten und Zusätzliche Entschlüsselungsschlüssel für ausgehende Nachrichten.

HINWEIS: Obwohl der Sicherheitsbeauftragte normalerweise nicht die ADKs verwenden sollte, ist dies möglicherweise erforderlich, um die E-Mail eines Benutzers wiederherzustellen. Dieser Fall tritt ein, wenn sich ein Benutzer beispielsweise verletzt und einige Zeit arbeitsunfähig ist, oder wenn E-Mails von Polizeipräsidien eingefordert werden und das Unternehmen Post als Beweismittel vor Gericht entschlüsseln muß.

PGP-Schlüsseln X.509-Zertifikate hinzufügen

HINWEIS: Dieser Vorgang ist von CA zu CA verschieden, und die zu verwendende Terminologie ist richtlinienabhängig. Für weitere Informationen hierzu müssen Sie sich möglicherweise an den PGP- oder PKI-Administrator Ihrer Firma wenden.

Ein digitales X.509-Zertifikat ist ein anerkanntes elektronisches Dokument zur Prüfung der Identität und der Eigentumsrechte öffentlicher Schlüssel in einem Kommunikationsnetzwerk.

Mit Hilfe der PGP-Menüoptionen und der *Zertifizierungsinstanz* (CA) Ihres Unternehmens oder einer öffentlichen CA (z. B. VeriSign) können Sie ein digitales X.509-Zertifikat anfordern und Ihrem Schlüsselpaar hinzufügen.

Das Hinzufügen eines X.509-Zertifikats zu einem Schlüsselpaar umfaßt die folgenden vier Hauptschritte:

1. Zunächst muß das Root-CA-Zertifikat bei der CA angefordert und Ihrem PGP-Schlüsselbund hinzugefügt werden (siehe Schritt 1).
2. Geben Sie dann auf der Registerkarte **CA-Optionen** die Angaben zur CA ein (siehe Schritt 2).
3. Fordern Sie von der CA ein Zertifikat an. Ihre X.509-Zertifikatsanforderung wird von der CA verifiziert und unterschrieben (siehe Schritt 3). (Durch die Unterschrift der CA auf dem Zertifikat ist es möglich, an den Identifizierungsinformationen oder dem öffentlichen Schlüssel vorgenommene Manipulationen festzustellen. Außerdem besagt die Unterschrift, daß die CA die im Zertifikat enthaltenen Informationen für gültig befindet.)
4. Rufen Sie das von der CA ausgestellte Zertifikat ab, und fügen Sie es Ihrem Schlüsselpaar hinzu (siehe Schritt 4).

Diese vier Schritte werden in den folgenden Abschnitten genauer beschrieben.

So fügen Sie Ihrem PGP-Schlüsselpaar ein X.509-Zertifikat hinzu:

1. Fordern Sie das Root-CA-Zertifikat an, und fügen Sie es Ihrem PGP-Schlüsselbund hinzu.

   Führen Sie hierzu die folgenden Schritte aus:

   a. Starten Sie Ihren Webbrowser, und stellen Sie eine Verbindung zur CA-Anmeldungssite her. Falls Ihnen die entsprechende URL nicht bekannt ist, erfragen Sie sie beim zuständigen PGP- bzw. PKI-Administrator.

   b. Gehen Sie zum Root-CA-Zertifikat, und prüfen Sie es. Dieser Vorgang ist von CA zu CA verschieden. Falls Ihr Unternehmen beispielsweise den Net Tools-PKI-Server verwendet, klicken Sie auf den Link **Herunterladen des CA-Zertifikats**, und klicken Sie dann auf **Untersuchung des Zertifikats**.

   c. Kopieren Sie den Schlüsselblock für das CA-Root-Zertifikat, und fügen Sie ihn in Ihr **PGPkeys**-Fenster ein.

      Das Dialogfeld “Schlüssel importieren” wird angezeigt, und das Root-CA-Zertifikat wird in Ihren Schlüsselbund importiert.

   d. Unterzeichnen Sie das Root-CA-Zertifikat mit Ihrem Schlüssel, um es gültig zu machen. Öffnen Sie dann das Dialogfeld “Schlüsseleigenschaften”, und legen Sie den Vertrauensgrad fest. Es muß ein Vertrauensgrad für die Root-CA eingestellt werden.

2. Konfigurieren Sie die auf der Registerkarte **CA-Optionen** vorhandenen Einstellungen.

   Führen Sie hierzu die folgenden Schritte aus:

   a. Wählen Sie den Befehl **Optionen** im PGPkeys-Menü **Bearbeiten**, und klicken Sie dann auf die Registerkarte **CA**.

      Die Registerkarte **CA** wird angezeigt (siehe Abbildung 4-10 auf Seite 93).

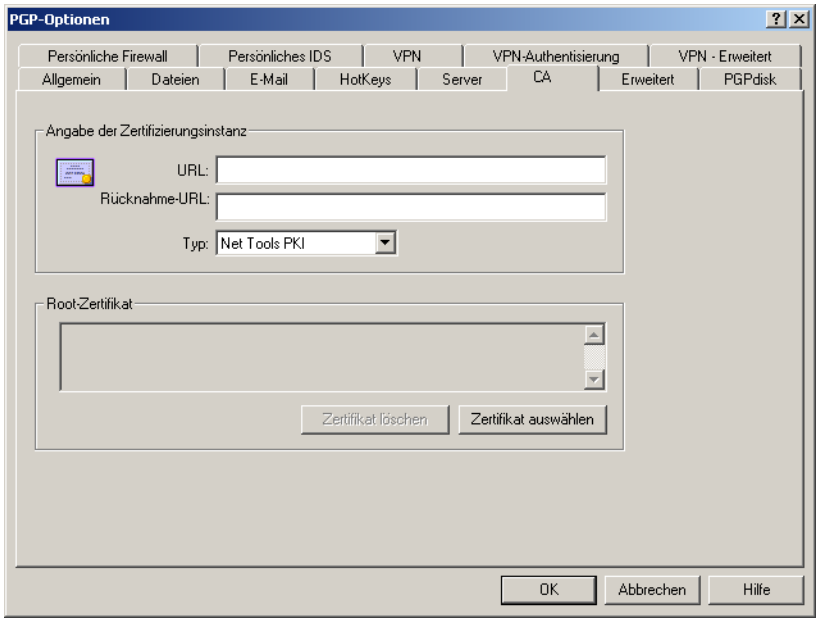


Abbildung 4-10. Dialogfeld “PGP-Optionen” (Registerkarte “CA”)

b. Geben Sie die URL der CA in das Textfeld **Zertifizierungsinstanz-URL** ein, also beispielsweise https://nnn.nnn.nnn.nnn:nnnnn (die gleiche URL, die Sie für die Anforderung der Root-CA verwendet haben).

c. Falls Sie über eine separate URL zur Anforderung von Listen zurückgenommener Zertifikate (CRL) verfügen, geben Sie diese in das zugehörige Textfeld ein.

   Falls Ihnen die URL zur Zurücknahme nicht bekannt ist, lassen Sie dieses Feld leer oder erfragen Sie sie beim zuständigen PGP- bzw. PKI-Administrator.

d. Geben Sie im Dialogfeld “Typ” den Namen Ihrer Zertifizierungsinstanz ein. Folgende Optionen stehen zur Verfügung:

   - Net Tools PKI
   - VeriSign OnSite
   - Entrust
   - iPlanet CMS
   - Windows 2000

e. Klicken Sie auf die Schaltfläche **Zertifikat auswählen**, und wählen Sie dann das gerade angeforderte Root-CA-Zertifikat aus.

Im Textfeld **Root-Zertifikat** werden Informationen zum ausgewählten Root-CA-Zertifikat angezeigt. Die Zertifikatsterminologie ist richtlinienabhängig. Normalerweise gilt für X.509-Zertifikate die folgende Terminologie:

Begriff:	Beschreibung:
CN (Common Name; Bekannter Name)	Häufig die Beschreibung des Zertifikatstyps (z. B. “Stamm”).
EMAIL	Die E-Mail-Adresse des Zertifikatsinhabers.
OU (Firmenabteilung)	Die Abteilung, der das Zertifikat zugeordnet ist (z. B. “Buchhaltung”).
O (Organisation)	Normalerweise der Name des Unternehmens, dem das Zertifikat zugeordnet ist (z. B. “Sicheres Unternehmen”).
L (Locality)	Standort des Inhabers des Zertifikats (z. B. “Berlin”)

f. Klicken Sie auf **OK**.

3. Fordern Sie ein Zertifikat an.

Führen Sie hierzu die folgenden Schritte aus:

a. Klicken Sie mit der rechten Maustaste auf Ihr PGP-Schlüsselpaar, und wählen Sie **Schlüssel—>Hinzufügen/Zertifikat** aus dem Kontextmenü.

Das Dialogfeld “Zertifikatsattribute” wird angezeigt (siehe Abbildung 4-11 auf Seite 95).

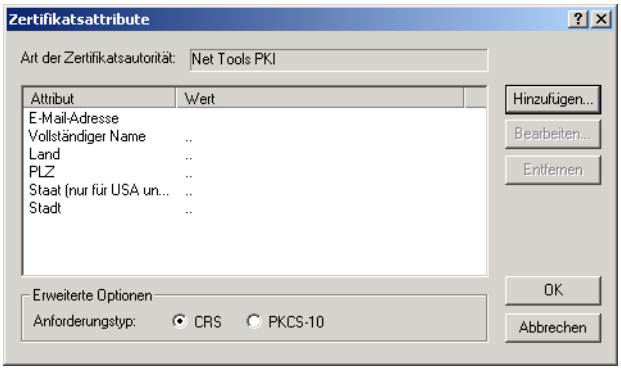


Abbildung 4-11. Dialogfeld “Zertifikatsattribute”

b. Verifizieren Sie die Zertifikatsattribute. Für etwaige Änderungen stehen Ihnen die Schaltflächen **Hinzufügen**, **Bearbeiten** und **Entfernen** zur Verfügung. Das Dialogfeld “PGP-Paßphrase eingeben” wird angezeigt.

c. Geben Sie die Paßphrase für Ihr Schlüsselpaar ein, und klicken Sie anschließend auf **OK**.

   Die Leiste zum **PGP-Server-Status** wird angezeigt.

   Die Zertifikatsanforderung wird an den CA-Server gesendet. Der Server authentisiert sich automatisch bei Ihrem Computer und nimmt Ihre Anfrage entgegen.

   Der PGP- bzw. PKI-Administrator Ihres Unternehmens überprüft die Informationen, die Sie in der Anfrage gemacht haben. Die Identifikationsinformationen und der öffentliche Schlüssel werden kombiniert und digital mit der eigenen Unterschrift der CA unterschrieben, um Ihr neues Zertifikat zu erstellen.

   Der Administrator sendet Ihnen daraufhin eine E-Mail mit dem Inhalt, daß Ihr Zertifikat abrufbereit ist.

4. Rufen Sie Ihr Zertifikat ab, und fügen Sie es Ihrem Schlüsselpaar hinzu.

   Es kann sein, daß Ihr Zertifikat automatisch abgerufen und Ihrem Schlüsselpaar hinzugefügt wird (abhängig von den durch den Administrator vorgenommenen Einstellungen). In diesem Fall können Sie mit Schritt c fortfahren.

Wenn das Zertifikat nicht automatisch abgerufen wird, können Sie es manuell abrufen und Ihrem Schlüsselbund hinzufügen. Führen Sie hierzu die folgenden Schritte aus:

a. Wählen Sie in PGPkeys den PGP-Schlüssel aus, für den Sie eine Zertifikatsanforderung erstellen möchten.

b. Wählen Sie im Menü **Server** den Befehl **Zertifikat abrufen**.

   PGP stellt eine Verbindung mit dem CA-Server her, um Ihr neues X.509-Zertifikat automatisch abzurufen und Ihrem PGP-Schlüssel hinzuzufügen.

c. Falls Sie PGPnet ausführen, stellen Sie dieses Zertifikat als Ihren X.509-Authentisierungsschlüssel in PGPnet ein (**Ansicht—>Optionen—>VPN-Authentisierung**)..

WICHTIG: Wenn Sie an Ihrem Schlüsselpaar Änderungen vornehmen bzw. diesem Informationen hinzufügen, müssen Sie stets das Schlüsselpaar auf dem Schlüsselserver aktualisieren, so daß allen die neueste Version Ihres Schlüssels zur Verfügung steht. Anweisungen dazu finden Sie im Abschnitt “Eigenen Schlüssel auf einem Schlüsselserver aktualisieren” auf Seite 104.

Schlüssel teilen und wieder zusammensetzen

Mit Hilfe eines Verschlüsselungsverfahrens, das als Blakely-Shamir-Splitting bezeichnet wird, kann jeder private Schlüssel in mehrere Teile für verschiedene “Halter” aufgeteilt werden. Die Verwendung dieses Verfahrens empfiehlt sich für Schlüssel mit sehr hoher Sicherheitsebene. Network Associates beispielsweise arbeitet mit einer Aufteilung von Schlüsseln auf mehrere Personen innerhalb der Firma. Wenn mit dem Schlüssel unterzeichnet werden muß, werden die Teile für die Dauer der Unterzeichnung wieder zusammengesetzt.

HINWEIS: Geteilte Schlüssel sind nicht mit PGP Desktop Security vor Version 6.0 bzw. mit PGP e-Business Server- und PGP-Befehlszeilen-Produkten vor Version 7.0 kompatibel.

Geteilten Schlüssel erstellen

Zum Aufteilen eines Schlüssels markieren Sie das gewünschte Schlüsselpaar, und wählen Sie im Menü **Schlüssel** den Befehl **Schlüsselaufteilung**. Sie werden dann aufgefordert, anzugeben, wie viele Teile für das Zusammensetzen des Schlüssels nötig sein sollen. Die Teile werden als Dateien gespeichert, die entweder mit dem öffentlichen Schlüssel eines der Halter oder, wenn der Halter über keinen öffentlichen Schlüssel verfügt, mit einem konventionellen Verschlüsselungsverfahren verschlüsselt werden. Bei Versuchen, mit dem geteilten Schlüssel zu unterschreiben oder zu entschlüsseln, versucht PGP automatisch, den Schlüssel wieder zusammenzusetzen. Informationen zum Zusammensetzen eines aufgeteilten Schlüssels finden Sie im Abschnitt “Dateien mit einem geteilten Schlüssel unterschreiben und entschlüsseln” auf Seite 132.

So teilen Sie einen Schlüssel in mehrere Teile:

1. Erstellen Sie zum Teilen in PGPkeys ein neues Schlüsselpaar, oder wählen Sie ein bereits vorhandenes Schlüsselpaar aus. Informationen dazu, wie Sie beim Erstellen eines neuen Schlüsselpaares vorgehen müssen, finden Sie im Abschnitt “Schlüsselpaare erstellen” auf Seite 42.

2. Klicken Sie im Menü **Schlüssel** auf **Schlüsselaufteilung**.

   Das Dialogfeld “Schlüsselaufteilung” wird angezeigt.

3. Weisen Sie dem Schlüsselpaar Schlüsselhalter zu, indem Sie deren Schlüssel aus PGPkeys in die Liste **Besitzer von Schlüsselteilen** des Dialogfelds “Schlüsselaufteilung” ziehen.

   Zum Hinzufügen eines Besitzers ohne öffentlichen Schlüssel klicken Sie im Dialogfeld “Schlüsselaufteilung” auf **Hinzufügen**, geben Sie den Namen der Person ein, und lassen Sie diese dann ihre Paßphrase eingeben.

4. Wenn alle Halter erfaßt sind, können Sie die Anzahl der Schlüsselteile angeben, die für das Entschlüsseln oder Unterschreiben mit diesem Schlüssel notwendig sind.

   Der Schlüssel in Abbildung 4-12 setzt sich beispielsweise aus insgesamt vier Teilen zusammen, und die Anzahl der für das Entschlüsseln oder Unterschreiben benötigten Schlüsselteile ist auf drei festgelegt. Damit wird ein Puffer geschaffen für den Fall, daß einer der Halter seinen Schlüsselteil nicht angeben kann oder seine Paßphrase vergessen hat.

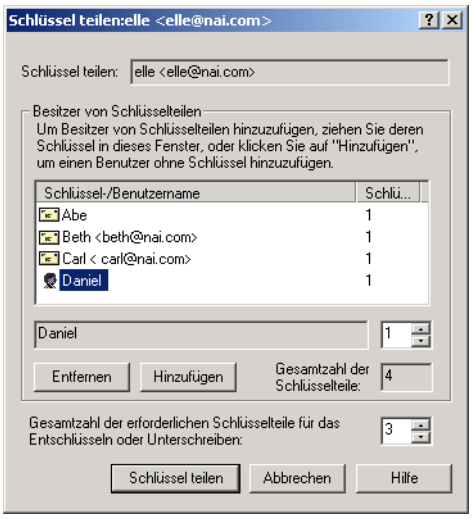


Abbildung 4-12. Dialogfeld “Schlüsselaufteilung” (Beispiel)

Standardmäßig ist jeder Halter für ein Schlüsselteil verantwortlich. Wenn Sie die Anzahl der im Besitz eines Halters befindlichen Teile erhöhen möchten, klicken Sie in der Liste der Besitzer auf den entsprechenden Namen, um ihn im Textfeld darunter anzuzeigen. Geben Sie die neue Anzahl der Schlüsselteile ein, oder wählen Sie mit Hilfe der Pfeile einen neuen Wert.

5. Klicken Sie auf **Schlüssel teilen**.

   Im angezeigten Dialogfeld werden Sie aufgefordert, ein Verzeichnis anzugeben, in dem die Teile abgelegt werden sollen.

6. Wählen Sie ein Verzeichnis zum Ablegen der Schlüsselteile.

   Das Dialogfeld “Paßphrase” wird angezeigt.

7. Geben Sie die Paßphrase für den Schlüssel ein, den Sie teilen möchten, und klicken Sie auf **OK**.

   Ein Dialogfeld zur Bestätigung des Vorgangs wird angezeigt.

8. Klicken Sie auf **Ja**, um den Schlüssel zu teilen.

   Der Schlüssel wird geteilt, und die Teile werden in dem angegebenen Verzeichnis gespeichert. Jedes Schlüsselteil wird mit dem Namen des Halters als Dateinamen und der Erweiterung .SHF (siehe Beispiel unten) gespeichert.

9. Verteilen Sie die Schlüsselteile an deren Besitzer, und löschen Sie dann die lokalen Kopien.

   Wenn ein Schlüssel auf mehrere Halter aufgeteilt wurde, versucht PGP bei Versuchen, mit dem geteilten Schlüssel zu unterschreiben oder zu verschlüsseln, automatisch, den Schlüssel wieder zusammenzusetzen. Hinweise dazu, wie Sie einen geteilten Schlüssel wieder zusammensetzen können, um damit Dateien zu unterschreiben oder zu entschlüsseln, finden Sie im Abschnitt “Dateien mit einem geteilten Schlüssel unterschreiben und entschlüsseln” auf Seite 132.

Geteilte Schlüssel zusammensetzen

Wenn ein Schlüssel auf mehrere Halter aufgeteilt wurde, versucht PGP bei Versuchen, mit dem geteilten Schlüssel zu unterschreiben oder zu verschlüsseln, automatisch, den Schlüssel wieder zusammenzusetzen. Sie können den Schlüssel lokal oder über das Netz wieder zusammensetzen.

Zum lokalen Zusammensetzen von Schlüsseln müssen die Halter von Schlüsselteilen an dem dafür vorgesehenen Computer anwesend sein. Jeder Halter von Schlüsselteilen muß die Paßphrase für seinen Schlüsselteil eingeben.

Beim Zusammensetzen der Schlüsselteile über das Netz müssen die Halter die Echtheit Ihrer Schlüssel bestätigen und diese entschlüsseln, bevor sie sie über das Netz schicken. Die TLS-Funktion (Transport Layer Security; TLS) von PGP gewährleistet die Sicherheit der Verbindung zur Übertragung der Schlüsselteile. Dadurch können mehrere Benutzer an verschiedenen Standorten mit ihrem Schlüsselteil ohne Risiko unterzeichnen und entschlüsseln.

WICHTIG: Vor Empfang der einzelnen Schlüsselteile über das Netz sollten Sie die Fingerabdrücke der einzelnen Halter überprüfen und deren jeweiligen öffentlichen Schlüssel unterschreiben, damit der Authentisierungsschlüssel legitim ist. Hinweise dazu, wie Sie Schlüsselpaare verifizieren können, finden Sie im Abschnitt “Mit digitalen Fingerabdrücken verifizieren” auf Seite 63.

So setzten Sie einen geteilten Schlüssel zusammen:

1. Kontaktieren Sie alle Halter des geteilten Schlüssels. Das lokale Zusammensetzen der Schlüsselteile setzt die Anwesenheit der Halter am entsprechenden Computer voraus.

   Zur Zusammenführung der Schlüsselteile über das Netz müssen alle Halter an den einzelnen Standorten PGP installiert haben und die entsprechenden Vorbereitungen für das Senden Ihrer Schlüsselteildatei getroffen haben. Folgende Vorbereitungen sind zu treffen:

   - Schlüsselteildateien und Paßwörter müssen verfügbar sein
   - es muß ein Schlüsselpaar existieren (zur Authentisierung für den Computer, auf dem die Schlüsselteile zusammengeführt werden)
   - eine Verbindung zum Netzwerk muß hergestellt sein
   - die IP-Adresse oder der Domänenname des Computers muß bekannt sein, auf dem die Schlüsselteile zusammengeführt werden

2. Wählen Sie auf dem für die Zusammenführung verwendeten Computer im Windows-Explorer die Dateien, die Sie mit dem geteilten Schlüssel unterzeichnen oder entschlüsseln möchten.

3. Klicken Sie mit der rechten Maustaste auf die Datei(en), und wählen Sie aus dem **PGP**-Menü den Befehl **Unterschreiben** oder **Entschlüsseln**.

   Das Dialogfeld “PGP – Eingabe der Paßphrase für ausgewählten Schlüssel” wird angezeigt. Der geteilte Schlüssel ist markiert.

4. Klicken Sie auf **OK**, um den ausgewählten Schlüssel wieder zusammenzusetzen.

   Das Dialogfeld “Sammlung der Schlüsselteile” wird angezeigt (siehe Abbildung 4-13).

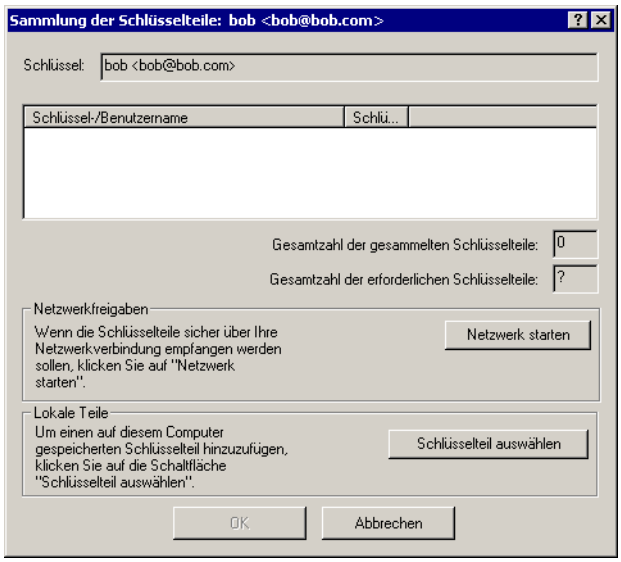


Abbildung 4-13. Dialogfeld “Sammlung der Schlüsselteile”

5. Führen Sie einen der folgenden Schritte aus:

   - **Wenn Sie die Schlüsselteile lokal zusammensetzen**, klicken Sie auf **Schlüsselteil auswählen**, und suchen Sie dann die mit dem geteilten Schlüssel verknüpften Schlüsselteile. Die Schlüsselteildateien können über die Festplatte, eine Diskette oder ein zugeordnetes Laufwerk zusammengesetzt werden. Fahren Sie mit Schritt 6 fort.

   - **Wenn Sie die Teile über das Netz zusammenführen**, klicken Sie auf **Netzwerk starten**.

     Das Dialogfeld “Paßphrase” wird angezeigt. Wählen Sie im Feld **Unterschriftenschlüssel** das Schlüsselpaar, das Sie für die Authentisierung beim entfernten System verwenden möchten, und geben Sie die Paßphrase ein. Klicken Sie auf **OK**. Der Computer wird auf den Empfang der Schlüsselteile vorbereitet.

     Der Status der Übertragung wird im Feld **Netzwerkfreigaben** angezeigt. Wenn der Status “Daten werden gelesen” angezeigt wird, ist PGP bereit, die Schlüsselteile zu empfangen.

Zu diesem Zeitpunkt müssen die Halter ihre Schlüsselteile abschicken. Anleitungen zum Senden der Schlüsselteile an den für die Zusammenführung verwendeten Computer finden Sie unter “So senden Sie Schlüsselteile über das Netzwerk:” auf Seite 103.

Wenn ein Schlüsselteil empfangen wurde, wird das Dialogfeld “Entfernte Authentisierung” angezeigt (siehe Abbildung 4-14).

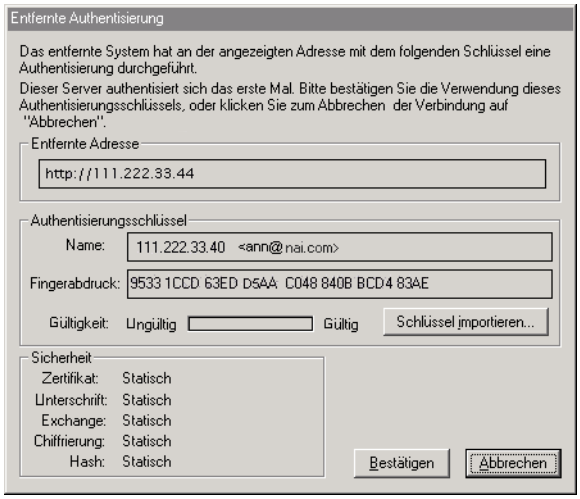


Abbildung 4-14. Dialogfeld “Entfernte Authentisierung”

Wenn Sie den Schlüssel, mit dem die Authentisierung des entfernten Systems durchgeführt wurde, nicht unterschrieben haben, ist der Schlüssel ungültig. Sie können die Teile zwar mit einem ungültigen Bestätigungsschlüssel zusammensetzen, dieser Vorgang empfiehlt sich jedoch nicht. Sie sollten die Fingerabdrücke der einzelnen Halter überprüfen und deren jeweiligen öffentlichen Schlüssel unterschreiben, um sicherzustellen, daß der Authentisierungsschlüssel legitim ist.

Klicken Sie zur Annahme des Schlüsselteils auf **Bestätigen**.

6. Sammeln Sie die übrigen Teile ein, bis der Wert unter **Gesamtzahl der gesammelten Schlüsselteile** dem Wert unter **Gesamtzahl der erforderlichen Schlüsselteile** im Dialogfeld “Sammlung der Schlüsselteile” entspricht.

7. Klicken Sie auf **OK**.

   Die Datei wird mit dem geteilten Schlüssel unterschrieben oder entschlüsselt.

So senden Sie Schlüsselteile über das Netzwerk:

1. Wenn sich die Person, die den geteilten Schlüssel wieder zusammensetzt, an Sie wendet, sollten Sie über folgende Elemente verfügen:
   - Ihre Schlüsselteildatei und Ihr Paßwort
   - Ihr Schlüsselpaar (zur Authentisierung für den Computer, auf dem die Schlüsselteile zusammengeführt werden)
   - eine Netzwerkverbindung
   - die IP-Adresse oder den Domänennamen des Computers, auf dem die Schlüsselteile zusammengeführt werden
2. Wählen Sie den Befehl **Schlüsselteile senden** aus dem PGPkeys-Menü **Datei**.

   Daraufhin wird das Dialogfeld **Schlüsselteil auswählen** angezeigt.
3. Gehen Sie zum Speicherort Ihres Schlüsselteils, und klicken Sie auf **Öffnen**.

   Das Dialogfeld “PGP-Paßphrase eingeben” wird angezeigt.
4. Geben Sie Ihre Paßphrase ein, und klicken Sie auf **OK**.

   Das Dialogfeld “Schlüsselteile senden” wird angezeigt (siehe Abbildung 4-15 auf Seite 103).

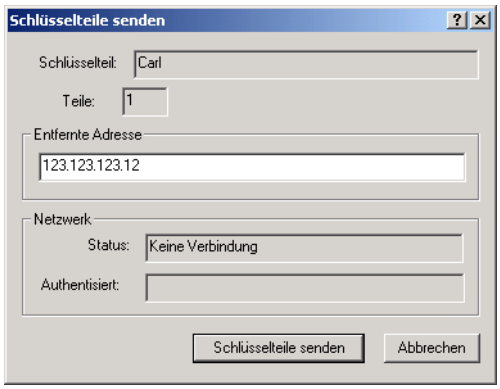


Abbildung 4-15. Dialogfeld “Schlüsselteile senden”

5. Geben Sie im Textfeld **Entfernte Adresse** die IP-Adresse oder den Domänennamen des Computers ein, auf dem die Teile wieder zusammengeführt werden, und klicken Sie dann auf **Schlüsselteile senden**.

   Der Status der Übertragung wird im Feld **Netzwerkstatus** angezeigt. Wenn dort "Verbindung hergestellt" angezeigt wird, werden Sie aufgefordert, sich für den Computer, auf dem die Teile zusammengeführt werden, zu authentisieren.

   Im angezeigten Dialogfeld "Entfernte Authentisierung" müssen Sie bestätigen, daß es sich bei dem entfernten Computer um den Computer handelt, an den Sie Ihren Schlüsselteil senden möchten.

6. Klicken Sie zur Fertigstellung der Übertragung auf **Bestätigen**.

   Wenn der Computer Ihre Schlüsselteile empfangen und deren Empfang bestätigt hat, wird ein Meldungsfeld mit einer Benachrichtigung über die erfolgreiche Übertragung der Teile angezeigt.

7. Klicken Sie auf **OK**.

8. Wenn Sie das Senden Ihres Schlüsselteils abgeschlossen haben, klicken Sie im Fenster **Schlüsselteile** auf **Fertig**.

Eigenen Schlüssel auf einem Schlüsselserver aktualisieren

Falls Sie Ihre E-Mail-Adresse ändern müssen oder neue Unterschriften verwenden, müssen Sie zum Ersetzen des alten Schlüssels lediglich eine Kopie des neuen Schlüssels an den Server senden. Die Server-Informationen werden dann automatisch aktualisiert. Sie sollten jedoch dabei bedenken, daß öffentliche Schlüsselserver nur in der Lage sind, neue Informationen hinzuzufügen und keine Entfernung von Benutzernamen oder Unterschriften aus Schlüsseln erlauben. Informationen dazu, wie Sie Unterschriften oder Benutzernamen von Ihrem Schlüssel entfernen können, finden Sie unter "Mit Ihrem Schlüssel verbundene Unterschriften oder Benutzernamen entfernen" auf Seite 105. Falls Ihr Schlüssel nicht mehr sicher ist, können Sie ihn zurücknehmen. Dadurch werden andere darüber informiert, daß dieser Schlüsselversion nicht mehr zu trauen ist. Genauere Informationen zum Zurücknehmen von Schlüsseln finden Sie im Abschnitt "Schlüssel zurücknehmen" auf Seite 90.

Mit Ihrem Schlüssel verbundene Unterschriften oder Benutzernamen entfernen

Bei Bedarf können Sie auch mit einem bestimmten Schlüssel verbundene Schlüssel, Unterschriften oder Benutzer-IDs löschen.

Öffentliche Schlüsselserver können ausschließlich neue Informationen hinzufügen, erlauben aber keine Entfernung von Benutzernamen oder Unterschriften aus Schlüsseln. Zum Entfernen von mit Ihrem Schlüssel verknüpften Unterschriften oder Benutzernamen müssen Sie zunächst den Schlüssel vom Server entfernen, die erforderliche Änderung vornehmen und dann den Schlüssel wieder auf dem Server ablegen.

Wenn aufgrund Ihrer PGP-Optionen / Server-Einstellungen eine Synchronisierung von Schlüsseln mit dem Schlüsselserver erfolgt, nachdem Ihrem Schlüssel Namen / Fotos / Rücknahmeschlüssel hinzugefügt wurden, wird Ihr Schlüssel automatisch auf dem Server aktualisiert. Falls dies einmal nicht geschehen sollte, befolgen Sie die nachstehenden Anweisungen, um Ihren Schlüssel manuell auf dem Schlüsselserver zu aktualisieren.

HINWEIS: Aus einem Schlüssel gelöschte Benutzernamen, Unterschriften und Schlüssel werden unwiederherstellbar entfernt. Unterschriften und Benutzernamen können einem Schlüssel aber erneut hinzugefügt werden, und ein importierter öffentlicher Schlüssel kann erneut in Ihren Schlüsselbund importiert werden. Ein privater Schlüssel jedoch, der nur an diesem Schlüsselbund vorhanden ist, kann nicht neu erstellt werden, und alle Nachrichten, die mit den Kopien des dazugehörigen öffentlichen Schlüssels verschlüsselt wurden, können nicht mehr entschlüsselt werden.

So entfernen Sie Unterschriften oder Benutzernamen von Ihrem auf einem Schlüsselserver abgelegten Schlüssel:

WICHTIG: Mit dieser Vorgehensweise können ausschließlich mit Ihrem Schlüssel verbundene Unterschriften oder Benutzernamen von LDAP-Schlüsselservern entfernt werden. Außerdem muß der Schlüsselserver für diesen Vorgang entsprechend konfiguriert sein. Falls Sie keine Informationen zum Servertyp oder dessen Konfigurationseinstellungen haben, wenden Sie sich an den Schlüsselserver-Administrator Ihres Unternehmens, bevor Sie Ihren Schlüssel aktualisieren.

---

1. Öffnen Sie PGPkeys.
2. Wählen Sie im Menü **Server** den Befehl **Suchen**, oder klicken Sie im PGPkeys-Menü auf .

   Daraufhin wird das PGPkeys-**Suchfenster** angezeigt.
3. Wählen Sie im Menü **Suche nach Schlüsseln in** den zu durchsuchenden Server aus.
4. Geben Sie für die Suche nach Ihrem öffentlichen Schlüssel Suchkriterien an:

   Standardmäßig ist **Benutzer-ID** ausgewählt, aber Sie können durch Klicken auf die Pfeile auch **Schlüssel-ID**, **Schlüsselstatus**, **Schlüsseltyp**, **Schlüsselgröße**, **Erstellungsdatum oder Gültigkeitsdatum** auswählen. Sie können beispielsweise alle Schlüssel mit der Benutzer-ID von Fred suchen.
5. Wenn Sie mit der Suche beginnen möchten, klicken Sie auf **Suchen**.

   Die Suchergebnisse werden im Fenster angezeigt.
6. Klicken Sie mit der rechten Maustaste auf den Schlüssel, den Sie vom Server entfernen möchten, und wählen Sie dann den Befehl **Löschen** aus dem Kontextmenü.

   Das Dialogfeld “Paßphrase” wird angezeigt.
7. Geben Sie die Paßphrase für den Schlüssel ein, den Sie vom Server entfernen möchten, und klicken Sie auf **OK**.

   Das Dialogfeld “Löschen bestätigen” wird angezeigt, und der Schlüssel wird entfernt.
8. Aktualisieren Sie Ihren Schlüssel (entfernen Sie die nicht länger gewünschten Unterschriften oder Benutzernamen).
9. Kopieren Sie den aktualisierten Schlüssel auf den Server (Hinweise dazu siehe “Eigenen öffentlichen Schlüssel auf einem Schlüsselserver ablegen” auf Seite 55).

   Wenn der Schlüsselserver so konfiguriert ist, daß die Schlüssel mit anderen Schlüsselservern synchronisiert werden, wird Ihr Schlüssel auf den anderen Servern automatisch bei der Synchronisierung aktualisiert.

WARNUNG: Falls Sie Ihren Schlüssel von einem Schlüsselserver löschen, sollten Sie bedenken, daß dieser öffentliche Schlüssel von einer anderen Person, die Ihren öffentlichen Schlüssel an Ihrem Schlüsselbund hat, wieder auf den Server übertragen werden kann. Überprüfen Sie den Server regelmäßig um sicherzustellen, daß der Schlüssel nicht erneut aufgenommen wurde. Möglicherweise müssen Sie einen Schlüssel also mehr als nur einmal vom Server löschen.

Schlüssel rekonstruieren

Wenn Sie Ihren privaten Schlüssel verlieren oder Ihre Paßphrase vergessen, können Ihre verschlüsselten Daten nicht wieder entschlüsselt werden, es sei denn, Ihr Administrator hat für Ihr Unternehmen die Möglichkeit der Schlüsselrekonstruktion eingerichtet. Dazu wurde ein Schlüsselrekonstruktionsserver eingerichtet und die entsprechende Option in Ihrer PGP-Software aktiviert. Wenn diese Funktion in Ihrer Software aktiviert wurde, haben Sie entsprechende Wiederherstellungsinformationen – fünf geheime Fragen und die entsprechenden Antworten – bereitgestellt und Ihren Schlüssel an den Schlüsselrekonstruktionsserver gesendet. Informationen dazu, wie Sie Ihren Schlüssel an einen Schlüsselrekonstruktionsserver senden können, finden Sie unter “So senden Sie Ihren Schlüssel an den Schlüsselrekonstruktionsserver Ihres Unternehmens:” auf Seite 53.

Befindet sich Ihr Schlüssel auf einem Rekonstruktionsserver, können Sie Ihr Schlüsselpaar jederzeit wiederherstellen. Dazu benötigen Sie Ihren öffentlichen Schlüssel, und Sie müssen in der Lage sein, mindestens drei der fünf von Ihnen festgelegten geheimen Fragen zu beantworten.

So rekonstruieren Sie Ihren Schlüssel vom Schlüsselrekonstruktionsserver Ihres Unternehmens:

1. Öffnen Sie PGPkeys, und wählen Sie den Schlüssel aus, den Sie rekonstruieren möchten.
2. Wählen Sie den Befehl **Schlüssel rekonstruieren** aus dem Menü **Schlüssel**.

   Wenn es sich bei dem Rekonstruktionsserver um einen PGP-Schlüsselserver handelt, wird das Dialogfeld “Benutzer-ID und Paßwort” angezeigt. Geben Sie zum Anmelden beim Server Ihre Benutzer-ID und das Paßwort ein. Wenn Sie Ihre Benutzer-ID bzw. Ihr Paßwort nicht kennen, wenden Sie sich an Ihren Administrator.
3. Klicken Sie auf **OK**.

   Das Dialogfeld “Schlüsselrekonstruktion” wird angezeigt.

4. Geben Sie in den **Antwortfeldern** des Dialogfelds “Schlüsselrekonstruktion” die Antworten auf die entsprechenden Fragen ein. Denken Sie daran, daß bei der Eingabe der Antworten auf die Groß- und Kleinschreibung zu achten ist. Um Ihren Schlüssel rekonstruieren zu können, müssen Sie mindestens 3 der 5 Fragen richtig beantworten können.

   Über die Option **Antworten verbergen** können Sie steuern, ob Ihre Antworten ein- oder ausgeblendet werden sollen.

5. Klicken Sie auf **OK**, um fortzufahren.

   Das Dialogfeld “PGP-Paßphrase eingeben” wird angezeigt.

6. Geben Sie im Feld **Paßphrase** eine neue Folge von Wörtern oder Zeichen ein, die als neue Paßphrase für Ihr neues Schlüsselpaar verwendet werden soll.

   HINWEIS: Ihre Paßphrase sollte aus mehreren Wörtern bestehen und kann Leerzeichen, Ziffern und Interpunktionszeichen enthalten. Denken Sie sich etwas aus, das Sie sich leicht merken können, aber das andere nicht erraten können. Bei der Paßphrase ist die Groß- und Kleinschreibung zu beachten, d. h., es wird zwischen großen und kleinen Buchstaben unterschieden. Je länger Ihre Paßphrase und je größer die Verschiedenheit der in ihr enthaltenen Zeichen ist, desto sicherer ist sie. In komplizierten Paßphrasen sind Groß- und Kleinbuchstaben, Ziffern, Satzzeichen und Leerzeichen enthalten. Solche Paßphrasen werden aber auch leichter vergessen. Weitere Informationen zur Auswahl einer Paßphrase finden Sie im Abschnitt “Einprägsame Paßphrasen erstellen” auf Seite 49.

   Drücken Sie zum Bestätigen Ihrer Eingabe die Tabulatortaste, um zur nächsten Zeile zu gelangen. Wiederholen Sie hier die Eingabe Ihrer Paßphrase.

7. Klicken Sie auf **OK**.

   Ihr Schlüsselpaar wird rekonstruiert und in PGPkeys angezeigt.

Teil III: Dateien, E-Mail-Nachrichten und Instantnachrichten sichern

- **Kapitel 5: E-Mail sichern**
- **Kapitel 6: Dateien sichern**
- **Kapitel 7: Instantnachrichten sichern**
- **Kapitel 8: Sichere Festplatten mit PGPdisk erstellen**

Sichere Kommunikation per E-Mail 5

PGP versetzt Sie in die Lage, mit Hilfe von Plugins und anderen Dienstprogrammen über Ihr E-Mail-Programm sicher zu kommunizieren. In diesem Kapitel wird beschrieben, wie Sie die zu versendenden E-Mail-Nachrichten verschlüsseln und unterschreiben sowie die empfangenen Nachrichten entschlüsseln und verifizieren können.

Sichere Kommunikation per E-Mail

Das Senden von unverschlüsselten E-Mail-Nachrichten ist so sicher wie das Versenden von Postkarten: Ihr Text kann in beiden Fällen von jedermann gelesen werden, der diese Nachricht auf dem Weg zum Empfänger “in die Hand” bekommt.

Mit PGP können Sie Ihre Nachrichten ganz einfach vor unberechtigtem Lesen schützen. Außerdem können Sie Ihren Nachrichten Ihre digitale Unterschrift hinzufügen und so deren Authentizität und Datenintegrität garantieren. Zum Sichern Ihrer E-Mails gibt es PGP-Plugins für die verschiedenen E-Mail-Programme sowie andere Dienstprogramme, mit denen Sie Ihren Nachrichtentext verschlüsseln und unterschreiben sowie entschlüsseln und verifizieren können. PGP-Plugins stehen für die folgenden E-Mail-Programme zur Verfügung: Microsoft Exchange, Outlook und Express, Lotus Notes sowie QUALCOMM Eudora.

PGP/MIME

Wenn Sie ein E-Mail-Programm mit einem der Plugins verwenden, das den PGP / MIME-Standard unterstützt, und Sie mit anderen Benutzern kommunizieren, deren E-Mail-Programm diesen Standard auch unterstützt, können beide Seiten beim Senden oder Abrufen der E-Mail-Nachrichten den Text der E-Mail-Nachricht und alle Dateianhänge automatisch ver- bzw. entschlüsseln. Hierzu müssen Sie nur im Dialogfeld “PGP-Optionen”, das Sie über PGPtray oder in PGPkeys öffnen können, die Funktionen für die PGP / MIME-Verschlüsselung und -Unterzeichnung aktivieren.

Wenn Sie eine E-Mail-Nachricht von einer Person erhalten, die die PGP / MIME-Funktion verwendet, ist diese E-Mail-Nachricht im Nachrichtenfenster mit einem Symbol versehen, das Ihnen anzeigt, daß sie mit PGP / MIME verschlüsselt wurde.

Doppelklicken Sie zum Entschlüsseln des Textes und der Dateianhänge in PGP / MIME-verschlüsselten E-Mail-Nachrichten sowie zum Verifizieren von digitalen Unterschriften einfach auf das Symbol mit dem Schloß und der Feder. Anhänge werden auch dann verschlüsselt, wenn PGP / MIME nicht verwendet wird; in diesem Fall ist es jedoch für den Empfänger zumeist aufwendiger, diese zu entschlüsseln.

E-Mail-Nachrichten verschlüsseln und unterschreiben

Die schnellste und einfachste Möglichkeit, E-Mail-Nachrichten zu verschlüsseln und zu unterschreiben, besteht darin, ein E-Mail-Programm zu verwenden, für das es ein PGP-Plugin gibt. Wenn Sie mit einem E-Mail-Programm arbeiten, für das es kein PGP-Plugin gibt, können Sie den Text Ihrer E-Mail-Nachrichten mit Hilfe von PGPtray oder PGPtools verschlüsseln,
unterschreiben, entschlüsseln und verifizieren.

E-Mail-Nachrichten mit den PGP-Plugins verschlüsseln und unterschreiben

Obwohl sich die Prozeduren in den verschiedenen E-Mail-Programmen etwas voneinander unterscheiden, wird die Verschlüsselung und das Unterschreiben bei allen Programmen durch Klicken auf die entsprechenden Schaltflächen in der Symbolleiste der jeweiligen Anwendung eingeleitet.

Wenn Sie Dateien mit einem E-Mail-Programm verschlüsseln und unterschreiben, für das es ein PGP-Plugin gibt, müssen Sie sich, abhängig vom Typ des vom Empfänger verwendeten E-Mail-Programms, für eines von zwei möglichen Verfahren entscheiden. Wenn Sie mit anderen PGP-Benutzern kommunizieren, die ein E-Mail-Programm verwenden, das den PGP / MIME-Standard unterstützt, können Sie mit Hilfe der PGP / MIME-Funktion Ihre E-Mail-Nachrichten und Dateianhänge beim Senden automatisch verschlüsseln und unterschreiben lassen. Arbeitet Ihr Kommunikationspartner mit einem E-Mail-Programm, das den PGP / MIME-Standard nicht unterstützt, sollten Sie vor dem Verschlüsseln Ihrer E-Mail-Nachrichten die PGP / MIME-Funktion deaktivieren, um Kompatibilitätsprobleme zu vermeiden. In Tabelle 5-1, “PGP-Plugin-Funktionen”, finden Sie eine Auflistung der verschiedenen Plugins und deren Funktionen.

TIP: Wenn Sie das E-Mail-Plugin, das Sie verwenden möchten, noch nicht installiert haben, führen Sie das Dienstprogramm “PGP Setup Maintenance” aus, und fügen Sie die zusätzlichen PGP-Komponenten und -Plugins hinzu. Nähere Informationen dazu finden Sie im Abschnitt “PGP-Installation bearbeiten” im PGP-Installationshandbuch.

Tabelle 5-1. PGP-Plugin-Funktionen

	Eudora	Outlook	Outlook Express	Lotus Notes
PGP/MIME	ja	nein	nein	nein
Automatisch entschlüsseln	nein	ja	ja	ja
HTML verschlüsseln	ja	ja	nein	ja
Textformatierung wird beibehalten	ja	ja	nein	ja
Anhänge werden verschlüsselt	ja	ja	nein	ja
Standardeinstellungen für Verschlüsseln/ Unterschreiben	ja	ja	ja	ja

So verschlüsseln und unterschreiben Sie Nachrichten mit unterstützten E-Mail-Programmen:

HINWEIS: Informationen dazu, wie Sie mit PGP Nachrichten unter Verwendung des Lotus Notes-Plugins verschlüsseln und unterschreiben können, finden Sie im Abschnitt “Nachrichten mit dem Lotus Notes-Plugin verschlüsseln und unterschreiben” auf Seite 117.

1. Erstellen Sie Ihre E-Mail-Nachricht wie gewohnt in Ihrem E-Mail-Programm.

TIP: Wenn Sie vertrauliche E-Mail-Nachrichten senden, sollten Sie in Ihre Betreffzeile nichts eingeben oder einen Betreff eintragen, durch den der Inhalt Ihrer verschlüsselten Nachricht nicht verraten wird.

2. Wenn Sie mit dem Verfassen des Textes Ihrer E-Mail-Nachricht fertig sind, klicken Sie auf das Symbol mit dem Umschlag und dem Schloß ( ), um den Text Ihrer Nachricht zu verschlüsseln. Danach können Sie die Nachricht durch Klicken auf das Symbol mit dem Papier und dem Stift ( ) unterschreiben.

HINWEIS: Wenn Sie PGP / MIME regelmäßig verwenden möchten, aktivieren Sie auf der Registerkarte **E-Mail** des Dialogfelds “PGP-Optionen” die entsprechenden Einstellungen.

---

3. Senden Sie Ihre Nachricht wie gewohnt.

   Wenn Sie für jeden Empfänger eine Kopie des öffentlichen Schlüssels haben, werden beim Senden automatisch die entsprechenden Schlüssel verwendet. Haben Sie jedoch einen Empfänger angegeben, von dem Sie keinen entsprechenden öffentlichen Schlüssel haben oder für den ein oder mehrere Schlüssel nicht über den ausreichenden Echtheitsgrad verfügen, wird das PGP-Dialogfeld “Empfängerauswahl” angezeigt (siehe Abbildung 5-1), in dem Sie den korrekten Schlüssel angeben können.

   Wenn dieses Dialogfeld auch dann angezeigt werden soll, wenn Sie eine gültige Kopie des öffentlichen Schlüssels der einzelnen Empfänger haben, halten Sie beim Klicken auf **Senden** die Umschalttaste gedrückt. Auf diese Möglichkeit sollten Sie zurückgreifen, wenn Sie die Option **Sichere Darstellung** bzw. **Konventionelle Verschlüsselung** verwenden möchten und nicht wollen, daß Ihre Nachricht automatisch versendet wird.

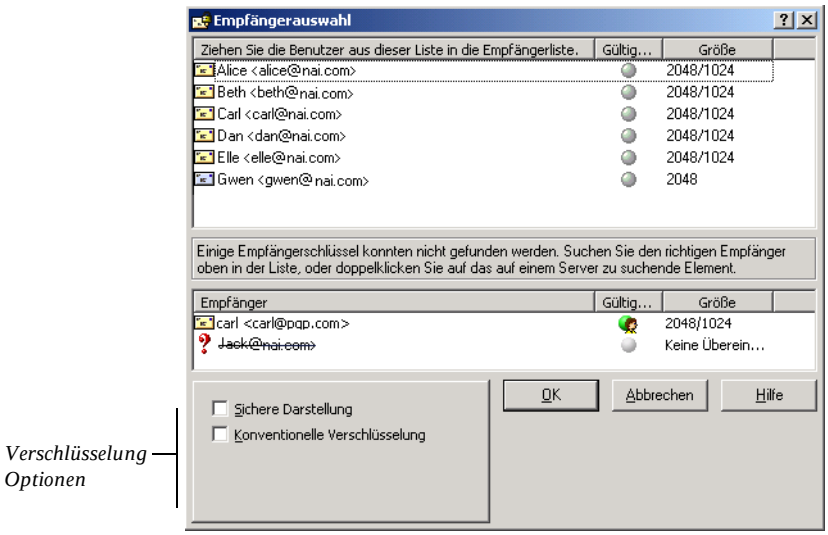


Abbildung 5-1. PGP-Fenster “Empfängerauswahl”

4. Ziehen Sie die öffentlichen Schlüssel der gewünschten Empfänger dieser verschlüsselten E-Mail-Nachricht in das Listenfeld **Empfänger**. Sie können auch auf jeden beliebigen Schlüssel doppelklicken, um ihn auf dem Bildschirm zu verschieben.

   Durch das Symbol **Gültigkeit** wird der Grad der Gewißheit angegeben, daß die öffentlichen Schlüssel in der Liste **Empfänger** echt sind. Diese Gültigkeit ergibt sich aus den mit dem Schlüssel verknüpften Unterschriften. Ausführliche Informationen dazu finden Sie in Kapitel 4, “Schlüssel verwalten”.

5. Abhängig vom Typ der zu verschlüsselnden Daten können Sie eine der folgenden Verschlüsselungsoptionen wählen:

   - **Sichere Darstellung:** Wenn Sie diese Option wählen, werden Daten bei der Entschlüsselung vor TEMPEST-Attacken geschützt. Die entschlüsselten Daten werden dann in einer speziellen Schriftart zur Verhinderung von TEMPEST-Attacken dargestellt, die nicht mit strahlungsempfindlichen Geräten aufgefangen werden kann. Weitere Informationen zu TEMPEST-Attacken finden Sie im Abschnitt zu Sicherheitsrisiken in der *Einführung in die Kryptographie*.

     HINWEIS: Die Option **Sichere Darstellung** ist möglicherweise nicht mit früheren PGP-Versionen kompatibel. Mit dieser Option aktivierte verschlüsselte Nachrichten können mit früheren PGP-Versionen entschlüsselt werden, wobei diese Funktion möglicherweise ignoriert wird.

   - **Konventionelle Verschlüsselung:** Wählen Sie diese Option, wenn Sie nicht mit öffentlichen Schlüsseln verschlüsseln, sondern eine gemeinsame Paßphrase verwenden möchten. Wenn Sie diese Option wählen, wird die Nachricht mit Hilfe eines Sitzungsschlüssels unter Verwendung einer Paßphrase verschlüsselt (und entschlüsselt). Sie werden aufgefordert, die zu verwendende Paßphrase zu wählen.

6. Klicken Sie auf **OK**, um Ihre Nachricht zu verschlüsseln und zu unterschreiben.

   Wenn Sie angegeben haben, daß Sie die verschlüsselten Daten unterschreiben möchten, wird vor dem Senden der Nachricht das Dialogfeld “Paßphrase des Unterschriftenschlüssels” angezeigt, in dem Sie dazu aufgefordert werden, Ihre Paßphrase einzugeben.

7. Geben Sie Ihre Paßphrase ein, und klicken Sie auf **OK**.

   WARNUNG: Wenn Sie Ihre E-Mail-Nachricht nicht sofort senden, sondern in Ihrem Postausgangsordner speichern, sollten Sie beachten, daß die Informationen bei einigen E-Mail-Programmen erst verschlüsselt werden, wenn die E-Mail-Nachricht tatsächlich gesendet wird. Bevor Sie verschlüsselte Nachrichten im Postausgangsordner ablegen, sollten Sie also überprüfen, ob Ihr Programm auch wirklich bereits die dort gespeicherten Nachrichten verschlüsselt. Ist dies nicht der Fall, können Sie Ihre Nachrichten mit der entsprechenden **Aktuelles Fenster**-Option in PGPtray vorher verschlüsseln.

Nachrichten mit dem Lotus Notes-Plugin verschlüsseln und unterschreiben

In diesem Abschnitt wird beschrieben, wie Sie E-Mail-Nachrichten mit dem PGP-Plugin für Lotus Notes verschlüsseln und unterschreiben können.

So verschlüsseln und unterschreiben Sie mit Lotus Notes:

1. Erstellen Sie mit Ihrem Lotus Notes-Client wie gewohnt Ihre E-Mail-Nachricht.

   TIP: Wenn Sie vertrauliche E-Mail-Nachrichten senden, sollten Sie in Ihre Betreffzeile nichts eingeben oder einen Betreff eintragen, durch den der Inhalt Ihrer verschlüsselten Nachricht nicht verraten wird.

2. Wenn Sie den Text Ihrer E-Mail-Nachricht vollständig eingegeben haben, klicken Sie auf die Schaltfläche **PGP** (

) in der Symbolleiste.

   Daraufhin öffnet sich ein Menü mit den PGP-Optionen (Abbildung 5-2).

Abbildung 5-2. PGP-Menü in Lotus Notes

3. Wählen Sie **Unterschreiben**, um Ihre Nachricht digital zu unterschreiben. Wählen Sie **Verschlüsseln**, um den Text Ihrer Nachricht zu verschlüsseln.

4. Wenn Sie sich für das Verschlüsseln der Nachricht entscheiden, haben Sie die Möglichkeit, auch den Text vor dem Senden zu verschlüsseln. Klicken Sie dazu auf die Schaltfläche **PGP**, und wählen Sie im neuen Menü den Befehl **Jetzt verschlüsseln!** (Abbildung 5-3).

Abbildung 5-3. PGP-Option “Jetzt verschlüsseln!”

5. Senden Sie Ihre E-Mail-Nachricht wie gewohnt.

6. Wenn Sie an Ihrem Schlüsselbund für jeden der Empfänger eine Kopie des öffentlichen Schlüssels haben, und der Name der Empfänger bzw. deren E-Mail-Adresse einer der Benutzer-IDs an Ihrem Schlüsselbund entspricht, werden die entsprechenden Schlüssel automatisch verwendet.

   Wenn jedoch der Empfängername bzw. die E-Mail-Adresse keiner der an Ihrem Schlüsselbund vorhandenen Benutzer-IDs entspricht, wenn Sie für einen Empfänger keinen entsprechenden öffentlichen Schlüssel an Ihrem Schlüsselbund haben oder wenn einer oder mehrere Schlüssel nicht über den ausreichenden Echtheitsgrad verfügen, wird das PGP-Dialogfeld “Empfängerauswahl” angezeigt (siehe Abbildung 5-1 auf Seite 115), in dem Sie den korrekten Schlüssel angeben können.

   Wenn dieses Dialogfeld auch dann angezeigt werden soll, wenn Sie eine gültige Kopie des öffentlichen Schlüssels der einzelnen Empfänger haben, halten Sie beim Klicken auf **Senden** die Umschalttaste gedrückt. Auf diese Möglichkeit sollten Sie zurückgreifen, wenn Sie die Option **Sichere Darstellung** bzw. **Konventionelle Verschlüsselung** verwenden möchten und nicht wollen, daß Ihre Nachricht automatisch versendet wird.

7. Ziehen Sie die öffentlichen Schlüssel der gewünschten Empfänger dieser verschlüsselten E-Mail-Nachricht in das Listenfeld **Empfänger**. Sie können auch auf jeden beliebigen Schlüssel doppelklicken, um ihn auf dem Bildschirm zu verschieben.

   Durch das Symbol **Gültigkeit** wird der Vertrauensgrad angegeben, daß die öffentlichen Schlüssel in der Liste **Empfänger** echt sind. Diese Gültigkeit ergibt sich aus den mit dem Schlüssel verknüpften Unterschriften. Ausführliche Informationen dazu finden Sie in Kapitel 4, “Schlüssel verwalten”.

8. Sie können Ihre E-Mail-Nachrichten auch konventionell verschlüsseln. Aktivieren Sie dazu die Option **Konventionelle Verschlüsselung**, wenn anstelle der Verschlüsselung mit einem öffentlichen Schlüssel eine gemeinsame Paßphrase verwendet werden soll. Wenn Sie diese Option wählen, wird die Nachricht mit Hilfe eines Sitzungsschlüssels unter Verwendung einer Paßphrase verschlüsselt (und entschlüsselt). Sie werden dabei aufgefordert, die zu verwendende Paßphrase zu wählen.

9. Klicken Sie auf **OK**, um Ihre Nachricht zu verschlüsseln und zu unterschreiben.

   Wenn Sie angegeben haben, daß Sie die verschlüsselten Daten unterschreiben möchten, wird vor dem Senden der Nachricht das Dialogfeld “Paßphrase des Unterschriftenschlüssels” angezeigt, in dem Sie dazu aufgefordert werden, Ihre Paßphrase einzugeben.

10. Geben Sie Ihre Paßphrase ein, und klicken Sie auf **OK**.

WARNUNG: Wenn Sie Ihre E-Mail-Nachricht nicht sofort senden, sondern in Ihrem Postausgangsordner speichern, sollten Sie beachten, daß die Informationen bei einigen E-Mail-Programmen erst verschlüsselt werden, wenn die E-Mail-Nachricht tatsächlich gesendet wird. Bevor Sie verschlüsselte Nachrichten im Postausgangsordner ablegen, sollten Sie also überprüfen, ob Ihr Programm auch wirklich bereits die dort gespeicherten Nachrichten verschlüsselt. Ist dies nicht der Fall, können Sie Ihre Nachrichten mit der entsprechenden **Aktuelles Fenster**-Option in PGPtray vorher verschlüsseln.

E-Mails ohne PGP-Plugins verschlüsseln und unterschreiben

Wenn es für Ihr E-Mail-Programm kein PGP-Plugin gibt, können Sie den Text Ihrer Nachricht vor dem Senden mit Hilfe von PGPtray bzw. PGPtools verschlüsseln. Am einfachsten lassen sich Ihre Nachrichten mit den **Aktuelles Fenster**-Optionen in PGPtray verschlüsseln.

So verschlüsseln und unterschreiben Sie E-Mails ohne ein PGP-Plugin:

1. Erstellen Sie Ihre E-Mail-Nachricht wie gewohnt mit Ihrem E-Mail-Programm.

   TIP: Wenn Sie vertrauliche E-Mail-Nachrichten senden, sollten Sie in Ihre Betreffzeile nichts eingeben oder einen Betreff eintragen, durch den der Inhalt Ihrer verschlüsselten Nachricht nicht verraten wird.

2. Wenn Sie den Text Ihrer E-Mail-Nachricht vollständig eingegeben haben, öffnen Sie PGPtray, und wählen Sie **Verschlüsseln**, **Unterschreiben** oder **Verschlüsseln/Unterschreiben** im Menü **Aktuelles Fenster**.

   Der verschlüsselte Text wird im Textbereich Ihres E-Mail-Programms angezeigt.

3. Fahren Sie mit Schritt 3 auf Seite 114 fort, um das Verschlüsseln und Unterschreiben abzuschließen.

E-Mail-Nachrichten für Empfängergruppen verschlüsseln

Mit PGP können Sie Gruppenverteilungslisten erstellen. Wenn Sie beispielsweise verschlüsselte E-Mail-Nachrichten an zehn Personen in der Gruppe “usergroup@nai.com” senden möchten, können Sie eine Verteilerliste mit diesem Namen erstellen. Das Menü **Gruppen** in PGPkeys enthält die Option **Gruppen anzeigen**, mit der das Fenster **Gruppen** ein- bzw. ausgeblendet werden kann. Wie das Fenster **Gruppen** aussieht, sehen Sie in Abbildung 5-4.

HINWEIS: Wenn Sie bestimmte Nachrichten für alle Mitglieder einer eingerichteten E-Mail-Verteilerliste verschlüsseln möchten, müssen Sie zuerst eine PGP-Gruppe erstellen, die denselben Namen aufweist und dieselben Mitglieder enthält wie die E-Mail-Verteilerliste. Wenn Sie beispielsweise in Ihrem E-Mail-Programm eine Liste mit dem Namen *usergroup@nai.com* eingerichtet haben, müssen Sie in PGP eine Gruppe mit dem Namen “usergroup@nai.com” erstellen.

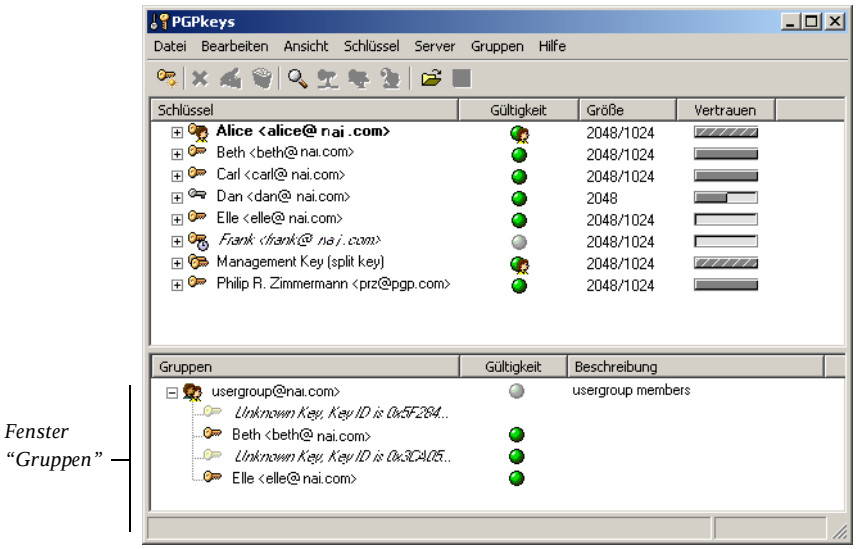


Abbildung 5-4. PGPkeys-Fenster “Gruppen”

Mit Verteilerlisten arbeiten

Mit der Funktion “Gruppen” können Sie Verteilerlisten erstellen und Listen von Empfängern bearbeiten, denen Sie verschlüsselte E-Mail-Nachrichten senden möchten.

So erstellen Sie eine Gruppe (Verteilerliste):

1. Wählen Sie **Neue Gruppe** aus dem Menü **Gruppen**.
2. Geben Sie einen Namen für die Gruppenverteilerliste ein. Wahlweise können Sie auch eine Beschreibung der Gruppe eingeben. Sie können beispielsweise die Gruppe “alle@nai.com” mit der Beschreibung “Alle Mitarbeiter” erstellen.
3. Klicken Sie auf **OK**, um die Verteilerliste zu erstellen.

   Die Gruppenverteilerliste wird Ihrem Schlüsselbund hinzugefügt und im Fenster **Gruppen** angezeigt.

So fügen Sie einer Verteilerliste neue Mitglieder hinzu:

1. Markieren Sie im PGPkeys-Fenster die Benutzer oder Listen, die Sie Ihrer Verteilerliste hinzufügen möchten.
2. Ziehen Sie die Benutzer aus dem PGPkeys-Fenster in die gewünschte Verteilerliste im Fenster **Gruppen**.

> **HINWEIS:** Mitglieder einer Verteilerliste können auch anderen Verteilerlisten hinzugefügt werden.

So löschen Sie Mitglieder aus einer Verteilerliste:

1. Markieren Sie in der Verteilerliste das zu löschende Mitglied.
2. Drücken Sie die ENTF-Taste.

   Danach werden Sie von PGP zur Bestätigung Ihrer Auswahl aufgefordert.

So löschen Sie eine Verteilerliste:

1. Markieren Sie im Fenster **Gruppen** die zu löschende Verteilerliste.
2. Drücken Sie die ENTF-Taste.

So fügen Sie eine Verteilerliste einer anderen Verteilerliste hinzu:

1. Markieren Sie die hinzuzufügende Verteilerliste.
2. Ziehen Sie die markierte Liste in die Liste, in die sie eingefügt werden soll.

Verschlüsselte und unterschriebene E-Mail-Nachrichten an Verteilerlisten senden

Nachdem Sie Ihre PGP-Verteilerlisten eingerichtet haben, können Sie an diese Empfängergruppen verschlüsselte E-Mail-Nachrichten senden. Weitere Informationen zum Erstellen und Bearbeiten von Verteilerlisten finden Sie im Abschnitt “Mit Verteilerlisten arbeiten” auf Seite 122.

So senden Sie verschlüsselte und unterschriebene E-Mail-Nachrichten an eine Verteilerliste:

1. Adressieren Sie die E-Mail-Nachricht an die Verteilerliste.

   Der Name Ihrer Verschlüsselungsverteilerliste muß mit dem Namen der E-Mail-Verteilerliste übereinstimmen.
2. Erstellen Sie Ihre E-Mail-Nachricht wie gewohnt mit Ihrem E-Mail-Programm.
3. Wenn Sie den Text Ihrer E-Mail-Nachricht vollständig eingegeben haben, öffnen Sie PGPtray, und wählen Sie **Verschlüsseln**, **Unterschreiben** oder **Verschlüsseln/Unterschreiben** im Menü **Aktuelles Fenster**.

   Das PGPkey-Dialogfeld “Empfängerauswahl” wird angezeigt (siehe Abbildung 5-1). Wählen Sie die öffentlichen Schlüssel der Personen aus, die die verschlüsselte oder unterschriebene Datei erhalten sollen. Weitere Informationen zu den verfügbaren Optionen finden Sie im Abschnitt “So verschlüsseln und unterschreiben Sie Nachrichten mit unterstützten E-Mail-Programmen:” auf Seite 113.
4. Senden Sie die Nachricht.

Entschlüsseln und Verifizieren von E-Mail-Nachrichten

Die schnellste und einfachste Möglichkeit, E-Mail-Nachrichten sicher auszutauschen, besteht darin, ein E-Mail-Programm zu verwenden, für das es ein PGP-Plugin gibt. Wenn Sie mit einem E-Mail-Programm arbeiten, für das es kein PGP-Plugin gibt, können Sie den Text Ihrer E-Mail-Nachrichten mit Hilfe von PGPtray oder PGPtools verschlüsseln, unterschreiben, entschlüsseln und verifizieren.

E-Mail-Nachrichten mit den PGP-Plugins entschlüsseln und verifizieren

Obwohl sich die Prozeduren in den verschiedenen E-Mail-Programmen etwas voneinander unterscheiden, wird die Entschlüsselung und das Verifizieren bei allen Programmen durch Klicken auf das Umschlagsymbol in der Nachricht bzw. in der Symbolleiste Ihres Programms eingeleitet. Gegebenenfalls müssen Sie in Ihrem E-Mail-Programm den Menübefehl **Entschlüsseln/ Verifizieren** wählen. Wenn Sie zudem mit einem Programm arbeiten, das den PGP/MIME-Standard unterstützt, können Sie sowohl Ihre E-Mail-Nachrichten als auch Dateianhänge entschlüsseln und verifizieren, indem Sie einfach auf ein Symbol klicken, das sich an Ihrer E-Mail-Nachricht befindet.

Wenn Sie mit einem E-Mail-Programm arbeiten, das nicht durch die PGP-Plugins unterstützt wird, können Sie Ihre E-Mail-Nachrichten mit PGPtray entschlüsseln und verifizieren. Wenn Ihre E-Mail-Nachricht zusätzlich verschlüsselte Dateianhänge enthält, müssen Sie diese mit PGPtools oder PGPtray separat entschlüsseln.

So entschlüsseln und verifizieren Sie Nachrichten in unterstützten E-Mail-Programmen:

HINWEIS: Informationen dazu, wie Sie mit dem Lotus Notes-Plugin Nachrichten entschlüsseln und verifizieren können, finden Sie im Abschnitt “Nachrichten mit dem Lotus Notes-Plugin entschlüsseln und verifizieren” auf Seite 125.

1. Öffnen Sie Ihre E-Mail-Nachricht wie gewohnt.

   Im Textkörper Ihrer E-Mail-Nachricht wird ein Block mit unlesbarem, chiffriertem Text angezeigt.

2. Klicken Sie auf das Symbol mit dem Briefumschlag und dem Schloß ( ), um die Nachricht zu entschlüsseln und zu verifizieren.

   Wenn Sie angehängte Dateien entschlüsseln und verifizieren müssen, entschlüsseln Sie diese separat mit PGPtools bzw. PGPtray.

   Das Dialogfeld “PGP-Paßphrase eingeben” wird angezeigt, und Sie werden zur Eingabe der Paßphrase aufgefordert.

3. Geben Sie Ihre Paßphrase ein, und klicken Sie auf **OK**.

   Die Nachricht wird entschlüsselt. Wenn die Nachricht unterschrieben wurde und Sie über den öffentlichen Schlüssel des Absenders verfügen, erhalten Sie eine Meldung darüber, ob die Unterschrift echt ist.

   Wenn beim Verschlüsseln der Nachricht die Option **Sichere Darstellung** aktiviert war, wird eine entsprechende Meldung angezeigt. Klicken Sie auf **OK**, um fortzufahren. Die entschlüsselte Nachricht wird in einem sicheren PGP-Bildschirm in einer speziellen Schriftart zur Verhütung von TEMPEST-Angriffen angezeigt.

4. Sie können die E-Mail-Nachricht im entschlüsselten Zustand speichern, oder Sie speichern die verschlüsselte Originalversion, damit sie weiterhin gesichert ist.

HINWEIS: Nachrichten, die verschlüsselt wurden, während die Option **Sichere Darstellung** aktiviert war, können nicht in entschlüsseltem Zustand gespeichert werden.

Nachrichten mit dem Lotus Notes-Plugin entschlüsseln und verifizieren

In diesem Abschnitt wird beschrieben, wie Sie E-Mail-Nachrichten mit dem Lotus Notes-PGP-Plugin entschlüsseln und verifizieren können.

So entschlüsseln und verifizieren Sie mit Lotus Notes:

1. Öffnen Sie Ihre E-Mail-Nachricht wie gewohnt.

   Im Textkörper Ihrer E-Mail-Nachricht wird ein Block mit unlesbarem, chiffriertem Text angezeigt.

2. Zum Entschlüsseln und Verifizieren der Nachricht klicken Sie auf die Schaltfläche **PGP Entschlüsseln/Verifizieren** (

) in der Symbolleiste.

   Wenn Sie angehängte Dateien entschlüsseln und verifizieren müssen, entschlüsseln Sie diese separat mit PGPtools bzw. PGPtray.

   Das Dialogfeld “PGP-Paßphrase eingeben” wird angezeigt, und Sie werden zur Eingabe der Paßphrase aufgefordert.

3. Geben Sie Ihre Paßphrase ein, und klicken Sie auf **OK**.

   Die Nachricht wird entschlüsselt. Wenn die Nachricht unterschrieben wurde und Sie über den öffentlichen Schlüssel des Absenders verfügen, erhalten Sie eine Meldung darüber, ob die Unterschrift echt ist.

4. Sie können die E-Mail-Nachricht im entschlüsselten Zustand speichern, oder Sie speichern die verschlüsselte Originalversion, damit sie weiterhin gesichert ist.

Nachrichten ohne PGP-Plugins entschlüsseln und verifizieren

Wenn es für Ihr E-Mail-Programm kein PGP-Plugin gibt, können Sie den Text Ihrer Nachricht mit Hilfe von PGPtray bzw. PGPtools entschlüsseln. Wenn Sie kein PGP-Plugin nutzen können, lassen sich Ihre Nachrichten am einfachsten mit den **Aktuelles Fenster**-Optionen von PGPtray entschlüsseln.

So entschlüsseln und verifizieren Sie Nachrichten in E-Mail-Programmen, für die es kein PGP-Plugin gibt:

1. Öffnen Sie Ihre E-Mail-Nachricht wie gewohnt.

   Im Textkörper Ihrer E-Mail-Nachricht wird ein Block mit unlesbarem, chiffriertem Text angezeigt.

2. Wählen Sie in PGPtray **Aktuelles Fenster—>Entschlüsseln/Verifizieren**.

   Wenn die E-Mail-Nachricht verschlüsselte Dateianhänge enthält, müssen Sie diese mit PGPtools oder PGPtray separat entschlüsseln.

   Das Dialogfeld **PGP-Paßphrase eingeben** wird angezeigt, in dem Sie zur Eingabe der Paßphrase aufgefordert werden.

3. Geben Sie Ihre Paßphrase ein, und klicken Sie auf **OK**.

   Die Nachricht wird entschlüsselt. Wenn sie unterschrieben wurde, erhalten Sie eine Meldung darüber, ob die Unterschrift echt ist.

   Wenn beim Verschlüsseln der Nachricht die Option **Sichere Darstellung** aktiviert war, wird eine entsprechende Meldung angezeigt. Klicken Sie auf **OK**, um fortzufahren. Die entschlüsselte Nachricht wird in einem sicheren PGP-Bildschirm in einer speziellen Schriftart zur Verhütung von TEMPEST-Angriffen angezeigt.

4. Sie können die E-Mail-Nachricht im entschlüsselten Zustand speichern, oder Sie speichern die verschlüsselte Originalversion, damit sie weiterhin gesichert ist.

HINWEIS: Nachrichten, die verschlüsselt wurden, während die Option **Sichere Darstellung** aktiviert war, können nicht in entschlüsseltem Zustand gespeichert werden.

Dateien sichern 6

In diesem Kapitel wird erläutert, wie Sie mit PGP Dateien sicher verwalten können. Sie finden hier Informationen dazu, wie Sie mit PGP Dateien zum Versenden als E-Mail-Nachrichten oder zur sicheren Aufbewahrung auf Ihrem Computer verschlüsseln, entschlüsseln, unterschreiben und verifizieren können. Darüber hinaus werden die PGP-Funktionen zum endgültigen Löschen von Dateien und zum Bereinigen des freien Speicherplatzes beschrieben, mit denen Dateien vollständig von Ihrem Computer gelöscht werden.

Dateien und Ordner mit PGP sichern

Mit PGP können Sie Dateien, die Sie als Anhang von E-Mails versenden möchten, verschlüsseln und unterschreiben, und Sie können Dateien bzw. Anhänge, die Ihnen verschlüsselt zugesandt wurden, entschlüsseln und verifizieren. Wie Sie diese PGP-Aufgaben ausführen können, wird in diesem Kapitel beschrieben.

Dateien verschlüsseln und unterschreiben

Zum Sichern Ihrer Dateien und Ordner stehen Ihnen die Optionen **Verschlüsseln**, **Unterschreiben** und **Verschlüsseln und Unterschreiben** in PGPtray, PGPtools bzw. im Windows-Explorer-Menü **Datei** zur Verfügung.

HINWEIS: Informationen dazu, wie Sie auf PGPtray, PGPtools bzw. das Menü **Datei** im Windows-Explorer zugreifen können, finden Sie in Kapitel 2, “Kurze Einführung in PGP”.

Wenn Sie den Befehl **Verschlüsseln** oder **Verschlüsseln und Unterschreiben** wählen, wird automatisch das PGP-Dialogfeld zur Schlüsselauswahl geöffnet (siehe Abbildung 6-1 auf Seite 130). In diesem Dialogfeld können Sie die öffentlichen Schlüssel der Empfänger für die zu verschlüsselnden Daten auswählen.

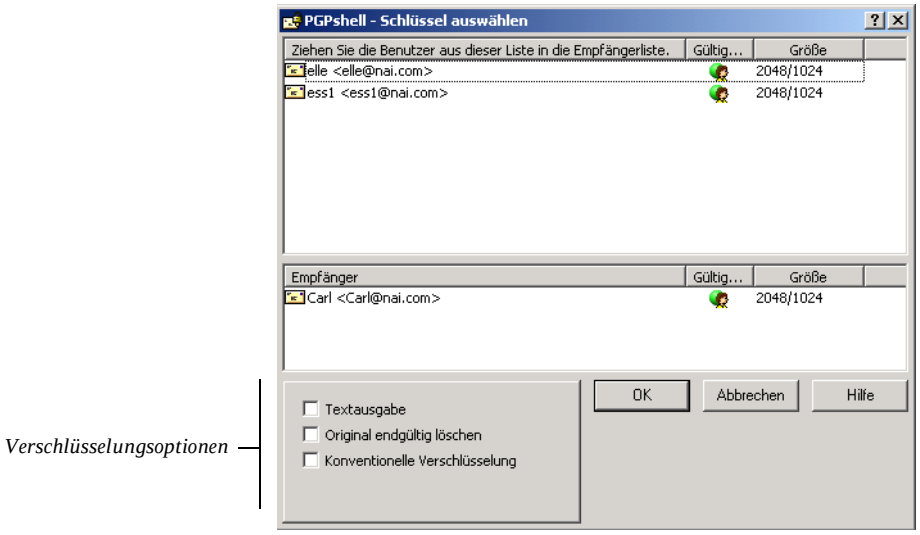


Abbildung 6-1. PGP-Dialogfeld zur Schlüsselauswahl

Auswählen können Sie diese öffentlichen Schlüssel, indem Sie sie in die Liste **Empfänger** ziehen. Sie können abhängig von dem Datentyp, den Sie verschlüsseln möchten, zusätzliche Verschlüsselungsoptionen aus dem Menü unten links auswählen. Folgende Optionen stehen hier zur Verfügung:

- **Textausgabe:** Wenn Sie Dateien als Anhänge senden, müssen Sie bei einigen E-Mail-Programmen möglicherweise die Option **Textausgabe** aktivieren, um die Datei als ASCII-Text speichern zu können. Bei älteren E-Mail-Programmen ist dies unter Umständen notwendig, wenn Sie eine Binärdatei senden möchten. Wenn Sie diese Option wählen, wird die Größe der verschlüsselten Datei um etwa 30 Prozent erhöht.
- **Original endgültig löschen:** Wenn Sie diese Option aktivieren, wird das verschlüsselte Originaldokument überschrieben, so daß Personen mit Zugriff auf Ihre Festplatte Ihre vertraulichen Informationen nicht lesen können.
- **Sichere Darstellung:** Aktivieren Sie diese Option, wenn Text beim Entschlüsseln vor TEMPEST-Angriffen geschützt werden soll. Die Daten werden dann in einer speziellen Schriftart zur Verhinderung von TEMPEST-Attacken dargestellt, die nicht mit strahlungsempfindlichen Geräten aufgefangen werden kann. Weitere Informationen zu TEMPEST-Attacken finden Sie im Abschnitt zu Sicherheitsrisiken in der *Einführung in die Kryptographie*. Diese Option ist nur verfügbar, wenn Sie Text oder Textdateien verschlüsseln.

- **Konventionelle Verschlüsselung:** Wählen Sie diese Option, wenn Sie eine allgemeine Paßphrase statt der Kryptographie mit öffentlichen Schlüsseln verwenden möchten. Die Datei wird mit Hilfe eines Sitzungsschlüssels unter Verwendung einer Paßphrase verschlüsselt (und entschlüsselt). Sie werden aufgefordert, die zu verwendende Paßphrase zu wählen.
- **Selbstentschlüsselnde Datei:** Wählen Sie diese Option, wenn Sie eine selbstentschlüsselnde ausführbare Datei erstellen möchten. Hierbei wird die Datei mit einem Sitzungsschlüssel verschlüsselt, der die Ver- und auch die Entschlüsselung mit einer angegebenen Paßphrase durchführt. Die erstellte ausführbare Datei kann entschlüsselt werden, indem man auf sie doppelklickt und die richtige Paßphrase eingibt. Diese Option ist besonders dann hilfreich, wenn verschlüsselte Dateien an eine Person verschickt werden sollen, die nicht über PGP verfügt. Dabei müssen der Absender und der Empfänger aber dasselbe Betriebssystem verwenden.

Wenn Sie die Dateien unterschreiben, werden Sie zur Eingabe Ihrer Paßphrase aufgefordert. Nach der Verschlüsselung wird im Ordner, in dem die Originaldatei gespeichert war, diese Datei mit dem angegebenen Namen sowie einem von drei möglichen Symbolen angezeigt:

verschlüsselt mit Textausgabe

verschlüsselt mit Standardausgabe

Ausgabe als selbstentschlüsselndes Archiv

Wenn Sie einen Ordner verschlüsseln oder unterschreiben, befindet sich die Ausgabe eventuell in einem neuen Ordner, abhängig von den gewählten Optionen.

Dateien entschlüsseln und verifizieren

Wenn Ihnen ein anderer Benutzer verschlüsselte Daten in einer Datei sendet, können Sie den Inhalt entschlüsseln und beigefügte Unterschriften verifizieren, um sicherzustellen, daß die Daten tatsächlich von dem angegebenen Absender stammen und nicht verändert wurden.

Verwenden Sie dazu den Befehl **Entschlüsseln/Verifizieren** in PGPtray, PGPtools bzw. im Menü **Datei** des Windows-Explorers.

HINWEIS: Informationen dazu, wie Sie auf PGPtray, PGPtools bzw. das Menü **Datei** im Windows-Explorer zugreifen können, finden Sie in Kapitel 2, “Kurze Einführung in PGP”.

Zum Entschlüsseln oder/und Verifizieren von Daten, die mit Ihrem Schlüssel verschlüsselt wurden, benötigen Sie Ihren privaten Schlüssel und Ihre Paßphrase. Wenn beim Verschlüsseln der Datei die Option **Sichere Darstellung** aktiviert war, wird der entschlüsselte Text zur Verhinderung von TEMPEST-Attacken in einer speziellen Schriftart und in einem sicheren PGP-Bildschirm angezeigt. War dies nicht der Fall, wird die Nachricht im Originalzustand angezeigt.

HINWEIS: Nachrichten, die verschlüsselt wurden, während die Option **Sichere Darstellung** aktiviert war, können nicht in entschlüsseltem Zustand gespeichert werden. Sie können erst nach der Entschlüsselung auf dem sicheren PGP-Bildschirm angezeigt werden.

Selbstentschlüsselnde Archive öffnen

Doppelklicken Sie zum Öffnen eines selbstentschlüsselnden Archivs (Self Decrypting Archive, SDA) auf die ausführbare Datei (diese sollte die Erweiterung .SDA.EXE haben). Geben Sie das richtige Paßwort ein, und legen Sie den Speicherort für die entschlüsselte Datei fest.

Dateien mit einem geteilten Schlüssel unterschreiben und entschlüsseln

Immer, wenn Sie Dateien mit einem geteilten Schlüssel unterschreiben oder entschlüsseln möchten, müssen Sie vorher den Schlüssel wieder zusammensetzen. Genaue Anweisungen dazu, wie Sie geteilte Schlüssel wieder einsammeln und zusammensetzen können, finden Sie im Abschnitt “Geteilte Schlüssel zusammensetzen” auf Seite 99.

Dateien unwiederbringlich löschen und Speicherplatz bereinigen

Wenn Sie auf Ihrem Computer wichtige Dateien erstellen und löschen, verbleiben Fragmente der in diesen Dateien enthaltenen Daten auf dem freien Speicherplatz Ihres Computers. Wenn Sie eine Datei wie üblich durch Verschieben in den Papierkorb löschen, wird nur der Name der Datei aus dem Dateiverzeichnis entfernt, die Daten der Datei verbleiben jedoch auf der Festplatte. Auch wenn Sie den Papierkorb dann leeren, werden die Daten erst komplett gelöscht, wenn das Betriebssystem den freien Speicherplatz überschreibt. Von vielen Programmen werden außerdem bei der Bearbeitung des Inhalts von Dokumenten temporäre Dateien erstellt. Diese Dateien werden beim Schließen der Dokumente gelöscht, aber Ihre Daten bleiben ebenfalls auf dem freien Speicherplatz zurück.

Im Klartext heißt das, daß Ihre wichtigen Dateien nie vollständig gelöscht werden und das jemand mit geeigneten Mitteln Ihre zuvor gelöschten Dateien wiederherstellen kann und von dem freien Speicherplatz auf Ihrem Computer auch an persönliche Informationen von Ihnen herankommen kann.

Wenn Sie solche wichtigen Dateien vollständig vernichten wollen, ohne daß Datenfragmente zurückbleiben, können Sie dies mit dem Dienstprogramm "PGP Wiper" tun. Wenn Sie Dateien mit der Funktion "Endgültig Löschen" löschen, werden diese (auch auf Systemen mit virtuellem Arbeitsspeicher) sofort überschrieben, und es werden auch sämtliche Spuren der Dateien entfernt, so daß diese auch nicht mit einem Datenwiederherstellungsprogramm wiederhergestellt werden können. Informationen dazu, wie Sie mit der Funktion "Endgültig löschen" Dateien löschen können, finden Sie im Abschnitt "Dateien mit der PGP-Funktion "Endgültig löschen" löschen" auf Seite 133.

Über **PGP-Optionen—> Allgemein** können Sie außerdem Einstellungen für das Endgültige Löschen von Dateien festlegen und die Funktion so konfigurieren, daß beim Löschen von Dateien diese automatisch sofort endgültig gelöscht werden. Hinweise, wie Sie diese Optionen aktivieren können, finden Sie im Abschnitt "Allgemeine Optionen festlegen" auf Seite 244.

Wenn Sie freien Speicherplatz bereinigen möchten, auf dem sich noch Daten zuvor gelöschter Dateien und Programme befinden, steht Ihnen dazu PGP Free Space Wiper zur Verfügung. Um sicherzustellen, daß Ihre gelöschten Daten nicht wiederherstellbar sind, empfehlen wir, Free Space Wiper in regelmäßigen Abständen auszuführen. Informationen dazu, wie Sie den freien Speicherplatz auf Ihrem Computer bereinigen können, finden Sie im Abschnitt "Mit dem PGP-Assistenten für das endgültige Löschen von freiem Speicherplatz arbeiten" auf Seite 134.

Dateien mit der PGP-Funktion "Endgültig löschen" löschen

Für das endgültige Löschen Ihrer Dateien und Ordner steht Ihnen die Option **Endgültig löschen** in PGPtools bzw. im Menü **Datei** des Windows-Explorers zur Verfügung.

HINWEIS: Informationen dazu, wie Sie auf PGPtools bzw. das Menü **Datei** im Windows-Explorer zugreifen können, finden Sie in Kapitel 2, "Kurze Einführung in PGP".

So löschen Sie Dateien und Ordner unwiederherstellbar:

1. Klicken Sie mit der rechten Maustaste auf die Datei, und wählen Sie aus dem Kontextmenü den Befehl Endgültig löschen, oder ziehen Sie die Datei in PGPtools auf die Schaltfläche **Endgültig löschen** ( ).

   Ein Dialogfeld zur Bestätigung des Vorgangs wird angezeigt.

2. Klicken Sie auf **OK**, wenn die Datei unwiederbringlich gelöscht werden soll.

   Wenn der Löschvorgang noch nicht beendet ist und Sie ihn anhalten möchten, klicken Sie auf **Abbrechen**.

HINWEIS: Durch Klicken auf **Abbrechen** während des Löschvorgangs bleiben eventuell Reste der Datei zurück.

WICHTIG: Beachten Sie, daß Dateien, die sich in Bearbeitung befinden, von vielen Programmen automatisch gespeichert werden und somit Sicherungskopien der gelöschten Datei vorhanden sein können. PGP Security, Inc. empfiehlt daher, daß Sie das Dienstprogramm “Endgültig löschen” sowohl für die Sicherungskopien als auch für die Originaldatei ausführen und diese so vollständig von der Festplatte entfernen.

Mit dem PGP-Assistenten für das endgültige Löschen von freiem Speicherplatz arbeiten

Den freien Speicherplatz auf Ihrer Festplatte können Sie mit der in PGPtools verfügbaren Option **Freien Speicherplatz endgültig löschen** bereinigen.

HINWEIS: Wie Sie PGPtools starten können, erfahren Sie in Kapitel 2, “Kurze Einführung in PGP”.

So bereinigen Sie den freien Speicherplatz auf Ihren Laufwerken:

1. Klicken Sie in PGPtools auf die Schaltfläche **Freien Speicherplatz endgültig löschen** ( ), um den Assistenten für das endgültige Löschen von freiem Speicherplatz zu starten.

   Das Begrüßungsfenster von **PGP Free Space Wiper** wird angezeigt.

2. Lesen Sie sich die angezeigten Informationen sorgfältig durch, und klicken Sie auf **Weiter**, um zum nächsten Dialogfeld zu gelangen.

   Sie werden aufgefordert, das zu bereinigende Volume und die Anzahl der dazu durchzuführenden Durchläufe anzugeben.

3. Wählen Sie im Feld **Laufwerk** die Festplatte bzw. das Volume, die bzw. das von PGP bereinigt werden soll. Wählen Sie anschließend die Anzahl der dazu durchzuführenden Durchläufe. Folgende Werte werden empfohlen:

   - 3 Durchläufe bei privater Nutzung.
   - 10 Durchläufe bei geschäftlicher Nutzung.
   - 18 Durchläufe bei militärischer Nutzung.
   - 26 Durchläufe für maximale Sicherheit.

   HINWEIS: Von professionellen Firmen, die sich mit der Wiederherstellung von Daten befassen, wurden schon Daten wiederhergestellt, die vorher neunmal überschrieben worden waren. PGP arbeitet in den einzelnen Durchläufen mit hochentwickelten Mustern, damit Ihre vertraulichen Daten unter keinen Umständen wiederhergestellt werden können.

   ---

4. Klicken Sie auf **Weiter**, um fortzufahren.

   Daraufhin wird das Dialogfeld “Löschvorgang ausführen” angezeigt, das statistische Angaben über das von Ihnen ausgewählte Laufwerk oder Volume enthält.

5. Klicken Sie auf die Schaltfläche **Löschvorgang beginnen**, um das Bereinigen des Laufwerks oder Volumes zu starten.

   Das Laufwerk oder Volume wird von PGP Free Space Wiper überprüft und anschließend von verbliebenen Fragmenten bereinigt.

6. Nach Abschluß der Bereinigung klicken Sie auf **Fertig stellen**.

WARNUNG: Durch Klicken auf **Abbrechen** während des Bereinigungsvorgangs bleiben eventuell Reste der Datei auf Ihrer Festplatte zurück.

Automatisches Bereinigen von Ordnern und freiem Speicherplatz einrichten

Für das Einrichten regelmäßiger automatischer Bereinigungen von Ordnern und freiem Speicherplatz steht Ihnen der Windows-Taskplaner zur Verfügung.

WICHTIG: Der Windows-Taskplaner muß auf Ihrem System installiert sein, damit Sie diese Planungsfunktion verwenden können. Sollte dies nicht der Fall sein, können Sie ihn von der Microsoft-Website (http://www.microsoft.com) herunterladen.

So planen Sie das Bereinigen von Ordnern und freiem Speicherplatz:

1. Wenn Sie festlegen möchten, daß Ihr freier Speicherplatz in regelmäßigen Abständen automatisch bereinigt werden soll, führen Sie die unter ”So bereinigen Sie den freien Speicherplatz auf Ihren Laufwerken:” beschriebenen Schritte 1 bis 4 aus. Wenn das Dialogfeld “Löschvorgang ausführen” angezeigt wird, klicken Sie auf die Schaltfläche **Planen**.

2. Wenn das Dialogfeld “Planen” angezeigt wird, klicken Sie auf **OK**, um fortzufahren.

   Unter Windows NT wird das Windows NT-Dialogfeld “Kennwort bestätigen” angezeigt.

   Geben Sie im ersten Textfeld Ihr Kennwort für die Anmeldung bei Windows NT ein. Drücken Sie die Tabulatortaste, um den Cursor in das nächste Textfeld zu setzen. Bestätigen Sie Ihre Eingabe, indem Sie Ihr Kennwort nochmals eingeben. Klicken Sie auf **OK**.

   Das Dialogfeld “Windows-Taskplaner” wird angezeigt (siehe Abbildung 6-2 auf Seite 137).

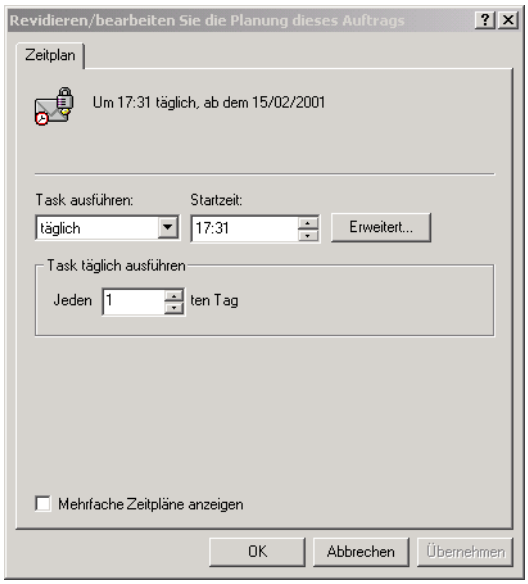


Abbildung 6-2. Registerkarte “Zeitplan” des Windows-Taskplaners

3. Wählen Sie aus, wie oft der entsprechende Task von dem Bereich **Task planen** aus ausgeführt werden soll. Folgende Optionen stehen zur Verfügung:

   - **Täglich**: Wenn Sie diese Option wählen, wird Ihr Task einmal zur angegebenen Zeit am angegebenen Tag ausgeführt. Klicken Sie auf **OK**, um das Dialogfeld zu schließen. Geben Sie dann im Textfeld Startzeit die Uhrzeit ein, zu der der Task täglich ausgeführt werden soll.

   - **Wöchentlich:** Wenn Sie diese Option wählen, wird Ihr Task am angegebenen Tag zur angegebenen Zeit wöchentlich ausgeführt. Geben Sie im entsprechenden Textfeld an, wie viele Wochen zwischen dem Bereinigen von Festplatten liegen sollen, und wählen Sie dann einen Tag in der Liste **Task wöchentlich ausführen**.

   - **Monatlich:** Wenn Sie diese Option wählen, wird Ihr Task am angegebenen Tag zur angegebenen Zeit einmal im Monat ausgeführt. Geben Sie im entsprechenden Textfeld die Uhrzeit und dann das Datum an, an dem der Task ausgeführt werden soll. Klicken Sie auf **Monate auswählen**, um anzugeben, in welchen Monaten der Task ausgeführt werden soll.

- **Einmal:** Wenn Sie diese Option wählen, wird Ihr Task am angegebenen Tag zur angegebenen Zeit genau einmal ausgeführt. Geben Sie die Uhrzeit an, und wählen Sie dann im Textfeld **Ausführen am** einen Monat und ein Datum aus.
- **Beim Systemstart:** Wenn Sie diese Option wählen, wird Ihr Task nur beim Starten des Computers ausgeführt.
- **Bei der Anmeldung:** Wenn Sie diese Option wählen, wird Ihr Task ausgeführt, wenn Sie sich bei Ihrem Computer anmelden.
- **Im Leerlauf:** Wenn Sie diese Option wählen, wird Ihr Task ausgeführt, sobald sich Ihr Computer für den angegebenen Zeitraum im Leerlauf befindet.

4. Geben Sie im Feld **Startzeit** die Uhrzeit an, zu der die Ausführung des Tasks gestartet werden soll.
5. Legen Sie im Feld **Task täglich ausführen** fest, wie oft der Task ausgeführt werden soll.
6. Klicken Sie auf **Erweitert**. Ein Dialogfeld wird geöffnet, in dem Sie zusätzliche Planungsoptionen wie das Start- und das Enddatum sowie die Dauer des Tasks festlegen können.
7. Klicken Sie auf **OK**.

   Ein Dialogfeld zur Bestätigung des Vorgangs wird angezeigt. Damit ist das Einrichten des automatischen Bereinigens von Ordnern und freiem Speicherplatz abgeschlossen. Wenn Sie Ihre PGP-Tasks bearbeiten oder löschen möchten, verwenden Sie den Windows-Taskplaner.

Instantnachrichten sichern 7

ICQ (“I seek you”) ist eine Internet-Anwendung, mit der Sie in Echtzeit mit Ihren Freunden und Kollegen über das Internet kommunizieren können. Wie bei jeder anderen Kommunikationsform auch, insbesondere bei der Kommunikation über Internet-basierte Anwendungen, ist Ihre Konversation nicht sicher und kann “belauscht” werden. Für eine sichere ICQ-Kommunikation bietet Ihnen PGP ein leistungsstarkes integriertes Plugin, mit dem Sie Ihre ICQ-Nachrichten schnell und problemlos ver- und entschlüsseln sowie Ihre PGP-Schlüssel über ICQ austauschen können.

Das PGP-Plugin für ICQ sorgt dafür, daß Ihre Nachrichten vor dem Senden über das Internet verschlüsselt und beim Öffnen von verschlüsselten Instantnachrichten diese automatisch entschlüsselt und verifiziert werden. Da das Plugin zum Verschlüsseln und Sichern Ihrer ICQ-Nachrichten Ihren PGP-Schlüssel und Ihre ICQ-Nummer verwendet, kann es auch automatisch die ICQ-Nachrichten, die mit Ihrem PGP-Schlüssel verschlüsselt wurden, entschlüsseln und verifizieren.

Wenn das PGP-Plugin für ICQ auf Ihrem System installiert ist, werden im ICQ-Dialogfeld “Send Online Message” das Symbol mit dem Schloß ( ) und die Schaltfläche **Send key** angezeigt (siehe Abbildung 7-1).

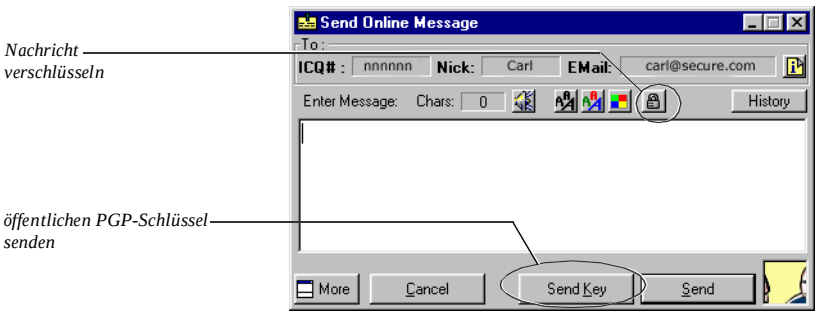


Abbildung 7-1. ICQ-Dialogfeld “Send Online Message”

Bevor Sie ICQ-Nachrichten verschlüsseln können, müssen Sie sich zunächst den öffentlichen Schlüssel der Person besorgen, der Sie die verschlüsselte Nachricht senden möchten. Der öffentliche Schlüssel des Empfängers kann ebenfalls über ICQ gesendet und mit Hilfe des ICQ-Plugins dem eigenen Schlüsselbund hinzugefügt werden. Anweisungen dazu finden Sie im Abschnitt “Öffentliche Schlüssel in ICQ austauschen” auf Seite 140.

Öffentliche Schlüssel in ICQ austauschen

Bevor Sie verschlüsselte Nachrichten über ICQ senden und empfangen können, müssen Sie mit allen Personen, mit denen Sie sicher korrespondieren möchten, die öffentlichen Schlüssel austauschen. Mit dem PGP-Plugin können Sie ICQ sowohl zum Senden und Empfangen der öffentlichen PGP-Schlüssel als auch zum Versenden von verschlüsselten Nachrichten verwenden.

WICHTIG: Mit ICQ ist es möglich, an Benutzer, die online sind, Nachrichten ohne jede Längenbegrenzung zu senden. Benutzer, die nicht online sind, können dagegen nur Nachrichten bis zu einer Länge von 450 Zeichen empfangen. Aufgrund dieser Beschränkung und angesichts der Tatsache, daß der verschlüsselte Text größer als der Ausgangstext werden kann, empfehlen wir, daß Sie Ihren Schlüssel und Ihre verschlüsselten Nachrichten nur an Empfänger senden, die online sind.

So senden Sie Ihren öffentlichen Schlüssel über ICQ:

1. Doppelklicken Sie in der Liste Ihrer ICQ-Kontakte auf den Namen der Person, der Sie Ihren öffentlichen Schlüssel senden möchten. Daraufhin wird das Dialogfeld “Send Online Message” geöffnet (siehe Abbildung 7-1).
2. Wenn Sie zusammen mit Ihrem Schlüssel eine Nachricht versenden möchten, geben Sie wie gewohnt den Text der Nachricht ein.
3. Klicken Sie auf die Schaltfläche **Send Key**.

   Ihr öffentlicher PGP-Schlüssel wird zusammen mit Ihrer ICQ-Nummer an den Empfänger gesendet.

HINWEIS: Der zusammen mit dem Schlüssel versendete Text wird nicht verschlüsselt.

So fügen Sie Ihrem Schlüsselbund über ICQ empfangene Schlüssel hinzu:

1. Öffnen Sie die Nachricht, die den PGP-Schlüssel enthält. Der öffentliche Schlüssel des Absenders wird im Textfeld des PGP-Dialogfelds “Schlüssel auswählen” angezeigt (siehe Abbildung 7-2).

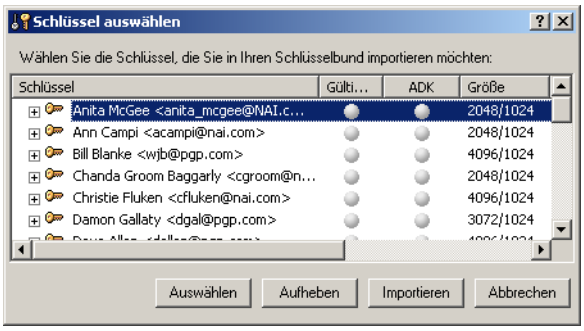


Abbildung 7-2. PGP-Dialogfeld “Schlüssel auswählen”

2. Wählen Sie den Schlüssel aus, und klicken Sie dann auf **Importieren**.

   Der Schlüssel wird Ihrem PGP-Schlüsselbund hinzugefügt.

ICQ-Nachrichten verschlüsseln

WICHTIG: Mit ICQ ist es möglich, Benutzern, die online sind, Nachrichten ohne jede Längenbegrenzung zu senden. Benutzer, die nicht online sind, können dagegen nur Nachrichten bis zu einer Länge von 450 Zeichen empfangen. Aufgrund dieser Beschränkung und angesichts der Tatsache, daß der verschlüsselte Text größer als der Ausgangstext werden kann, empfehlen wir, daß Sie Ihren Schlüssel und Ihre verschlüsselten Nachrichten nur an Empfänger senden, die online sind.

So senden Sie verschlüsselte ICQ-Nachrichten:

1. Tauschen Sie mit den Personen, denen Sie verschlüsselte Nachrichten senden bzw. von denen Sie verschlüsselte Nachrichten empfangen möchten, den öffentlichen Schlüssel aus. Informationen, wie Sie beim Austauschen von Schlüsseln über ICQ vorgehen müssen, finden Sie im Abschnitt ”Öffentliche Schlüssel in ICQ austauschen”.

2. Verfassen Sie Ihre Nachricht wie gewohnt.

   HINWEIS: Beim Verschlüsseln der Nachricht gehen die in ICQ vorgenommenen Formatierungen verloren.

3. Wenn Sie mit dem Verfassen der Nachricht fertig sind, klicken Sie auf das Symbol mit dem Schloß ( ) im ICQ-Dialogfeld “Send Online Message” (siehe Abbildung 7-1).

   Der Text der Nachricht wird verschlüsselt.

4. Klicken Sie auf **Send**.

Sichere Festplatten mit PGP-disk erstellen 8

In diesem Kapitel werden das Modul PGPdisk und seine Funktionen beschrieben sowie Hinweise zur Benutzung von PGPdisk gegeben.

PGPdisk-Grundlagen

PGPdisk ist eine Anwendung zum Verschlüsseln, die leicht zu bedienen ist und mit der Sie einen Bereich Ihrer Festplatte für die Speicherung vertraulicher Daten reservieren können. Dieser Bereich wird zum Erstellen einer Datei verwendet, die als PGPdisk-*Volume* bezeichnet wird.

Obwohl es sich nur um eine Datei handelt, funktioniert ein PGPdisk-Volume in etwa wie eine Festplatte, da es Speicherplatz für Ihre Dateien und Anwendungen zur Verfügung stellt. Sie können es sich ungefähr wie eine Diskette oder eine externe Festplatte vorstellen. Wenn Sie die im Volume gespeicherten Anwendungen und Dateien verwenden möchten, müssen Sie das Volume *laden*, d. h. für Sie zugänglich machen.

Danach können Sie mit einem PGPdisk-Volume wie mit jeder anderen Festplatte auch arbeiten. Sie können auf dem Volume Anwendungen installieren oder Ihre Dateien in das Volume verschieben oder dort speichern. Wenn das Volume *entladen* wird, kann es nur noch von Benutzern aufgerufen werden, die Ihre geheime Paßphrase kennen. (Weitere Informationen zu Paßphrasen finden Sie im Abschnitt “Einprägsame Paßphrasen erstellen” auf Seite 49). Auch ein geladenes Volume ist geschützt; sofern keine Datei oder Anwendung geöffnet ist, wird es in verschlüsselter Form gespeichert. Sollte Ihr Computer abstürzen, während ein Volume geladen ist, bleibt der Inhalt des Volumes verschlüsselt.

PGPdisk-Funktionen

PGPdisk bietet die folgenden Möglichkeiten:

- Erstellen von geschützten Volumes mit verschlüsselten Daten, die genauso wie die bereits vertrauten Volumes zum Speichern von Dateien funktionieren
- schnelle und sichere Verschlüsselung Ihrer Daten mit minimaler Verzögerung beim Öffnen Ihrer Programme und Dateien

- Speichern des Inhalts aller geschützten Volumes in einer verschlüsselten Datei, von der problemlos Sicherheitskopien erstellt werden können und die mit Kollegen ausgetauscht werden kann.
- zwei leistungsstarke Algorithmusoptionen zum Schutz Ihrer PGPdisk-Volumes:
  - **CAST5-Verschlüsselungsalgorithmus (128 Bit):** CAST ist eine 128-Bit-Blockverschlüsselung, die mit einem zuverlässigen, für militärische Zwecke geeigneten Verschlüsselungsalgorithmus arbeitet. Dieser ist für seine Fähigkeit bekannt, unberechtigte Zugriffe wirksam zu verhindern.
  - **Twofish-Verschlüsselungsalgorithmus (256 Bit):** Twofish ist ein neuer, von Bruce Schneier entwickelter symmetrischer 256-Bit-Blockverschlüsselungsalgorithmus. Er ist einer von fünf Algorithmen, die vom US-amerikanischen National Institute of Standards and Technology (NIST) für den Advanced Encryption Standard (AES) in Betracht gezogen werden, der den Data Encryption Standard (DES) ersetzt.

Sinn und Zweck von PGPdisk

Der Zugriff auf Dateien wird bei anderen Produkten durch Zugriffsattribute und einfache Paßwörter geregelt. Damit sind Ihre vertraulichen Daten allerdings nicht uneingeschränkt geschützt. Erst durch Verschlüsseln Ihrer Daten können Sie sicher sein, daß der Inhalt Ihrer Dateien selbst durch die modernste Technik nicht entschlüsselt werden kann.

In der folgenden Liste finden Sie einige Gründe für die Verwendung von PGPdisk zum Sichern Ihrer Dateien:

- Schutz von vertraulichen finanziellen, medizinischen und persönlichen Daten, auf die andere keinen Zugriff haben sollen. Dies ist besonders in der heutigen Internetumgebung wichtig, in der Informationen auf Ihrem PC für die ganze Welt zugänglich sind, wenn Sie im Internet surfen.
- Einrichten von persönlichen Arbeitsbereichen auf einem gemeinsam genutzten Rechner, auf dem jedem Benutzer ein exklusiver Zugriff auf seine Programme und Dateien garantiert wird. Jeder Benutzer kann seine eigenen Volumes laden, während er mit dem Rechner arbeitet. Nach dem Entladen kann er dann sicher sein, daß niemand unbefugt auf seine Dateien zugreifen kann.

- Erstellen von Volumes mit Daten, die nur festgelegten Mitgliedern einer bestimmten Arbeitsgruppe zugänglich sind. Ein Volume kann geladen werden, wenn Mitglieder des Teams an einem bestimmten Projekt arbeiten möchten. Nach der Arbeit kann es wieder entladen und im verschlüsselten Format gespeichert werden.
- Schutz vor unberechtigtem Zugriff auf die auf einem Notebook-Computer gespeicherten Informationen. Wenn Sie Ihr Notebook verlieren (oder es gestohlen wird), können Ihre gesamten persönlichen Daten (einschließlich Zugriff auf Online-Dienste und zugehörige Paßwörter, Daten über Geschäftspartner und Bekannte, finanzielle Daten usw.) von den Dieben mißbraucht werden, was zu Verlustkosten führen kann, die höher als die des Notebooks selbst sind.
- Sichern des Inhalts von externen Medien, wie beispielsweise von Disketten und Magnetbändern. Die Möglichkeit des Verschlüsselns von externen Medien bietet einen zusätzlichen Schutz beim Speichern und Austauschen von vertraulichen Informationen.

Kurze Einführung in PGPdisk

In diesem Abschnitt erhalten Sie einen kurzen Überblick über die Benutzeroberfläche von PGPdisk. Die meisten PGPdisk-Operationen können von Ihrem Windows-Explorer-Fenster, von PGPtray oder von einem PGPdisk-Editor aus ausgeführt werden.

Auf PGPdisk zugreifen

Sie können auf PGPdisk über das **Startmenü** oder über **PGPtray** zugreifen. Informationen dazu, wie Sie PGPdisk starten und ein neues PGPdisk-Volume erstellen können, finden Sie im Abschnitt "Neues PGPdisk-Volume erstellen" auf Seite 150.

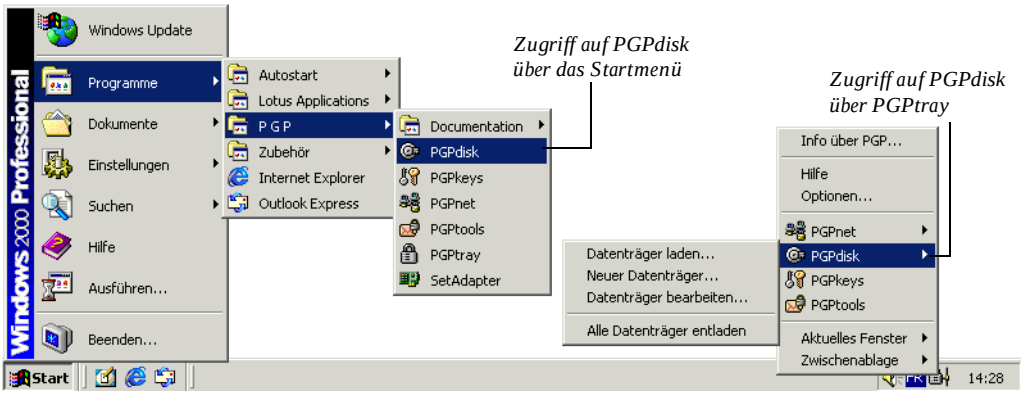


Abbildung 8-1. Auf PGPdisk zugreifen

Mit Hilfe des PGPdisk-Menüs, das Sie über PGPtray aufrufen können, lassen sich Volumes einfach erstellen und laden. Im folgenden finden Sie eine kurze Beschreibung der einzelnen Menübefehle:

Befehl:	Beschreibung:
Datenträger laden	Lädt das angegebene PGPdisk-Volume, wenn die Paßphrase korrekt eingegeben wurde.
Neuer Datenträger	Öffnet den PGPdisk-Assistenten, der Sie Schritt für Schritt durch den Prozeß des Erstellens eines neuen PGPdisk-Volumes führt.
Datenträger bearbeiten	Öffnet den PGPdisk-Editor, in dem Sie administrative Aufgaben an PGPdisk-Volumes ausführen können.
Alle Datenträger entladen	Entlädt alle vorhandenen PGPdisk-Volumes und speichert sie in verschlüsseltem Format.

Mit PGPdisk in einem Windows-Explorer-Fenster arbeiten

Im Windows-Explorer-Fenster (siehe Abbildung 8-2 auf Seite 147) können Sie die wichtigsten PGPdisk-Operationen ausführen, wie beispielsweise:

- PGPdisk-Volumes laden
- geladene PGPdisk-Volumes entladen
- auf Ihrem PGPdisk-Volume gespeicherte Dateien und Ordner erstellen, kopieren, verschieben und löschen
- PGPdisk-Editor für ein PGPdisk-Volume öffnen

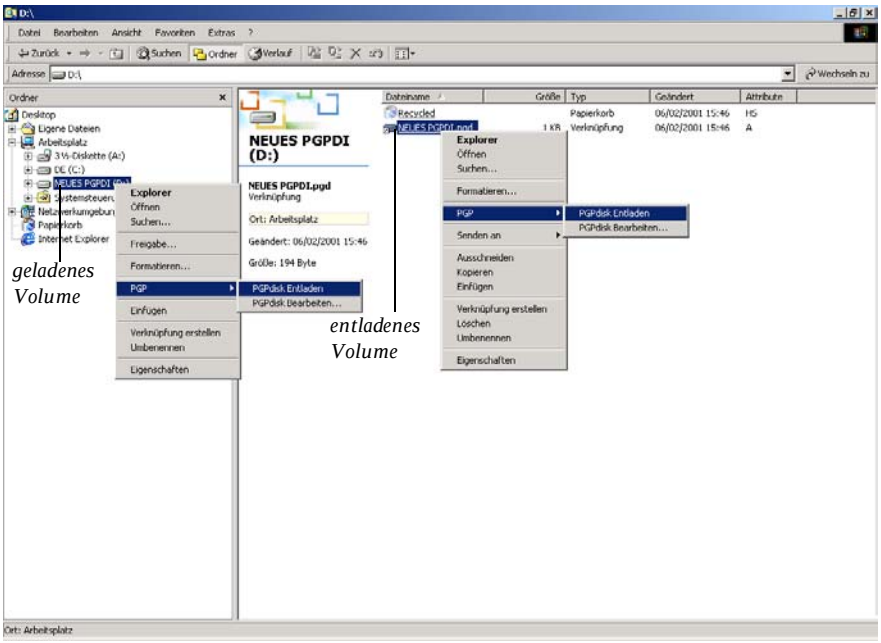


Abbildung 8-2. Im Windows-Explorer arbeiten

Wenn ein Volume entladen wurde, ist der Inhalt des Volumes in einer verschlüsselten Datei gespeichert und erst wieder zugänglich, wenn das Volume wieder geladen wird. Die `.pgd`-Datei mit dem PGPdisk-Inhalt kann auf einer Festplatte Ihrer Wahl in Ihrem System gespeichert werden. Dabei steht das Symbol für eine entladene PGPdisk-Volumedatei.

Nachdem ein PGPdisk-Volume geladen wurde, wird es im Windows-Explorer-Fenster sofort als leeres Laufwerk angezeigt, so daß Sie unmittelbar damit arbeiten können (siehe Abbildung 8-2 auf Seite 147).

So laden Sie ein PGPdisk-Volume im Windows-Explorer:

1. Wählen Sie in der Verzeichnishierarchie im Windows-Explorer die verschlüsselte Volumedatei aus, die Sie laden möchten.
2. Klicken Sie mit der rechten Maustaste auf den Namen der verschlüsselten Volumedatei. Daraufhin wird das Kontextmenü angezeigt.
3. Wählen Sie **PGP—>PGPdisk laden**.
4. Geben Sie die Paßphrase ein, und klicken Sie auf **OK**.

So entladen Sie ein PGPdisk-Volume im Windows-Explorer:

1. Wählen Sie in der Verzeichnishierarchie im Windows-Explorer die Volumedatei aus, die Sie entladen möchten.
2. Klicken Sie mit der rechten Maustaste auf den Namen der geladenen Volumedatei. Daraufhin wird das Kontextmenü angezeigt.
3. Wählen Sie **PGP—>PGPdisk Entladen**.

So arbeiten Sie mit PGPdisk in einem PGPdisk-Editor

Der PGPdisk-Editor dient zur Verwaltung des PGPdisk-Volumes. Folgende Aufgaben können im PGPdisk-Editor ausgeführt werden:

- Paßphrase ändern
- alternative Benutzer hinzufügen und entfernen
- Schreibschutz festlegen
- PGPdisk-Volumes laden
- geladene PGPdisk-Volumes entladen
- PGP-Optionen festlegen
- Festlegen der PGP-Eigenschaften, so daß Ihr PGPdisk-Volume beim Starten des Computers geladen bzw. Ihr Volume neu verschlüsselt wird

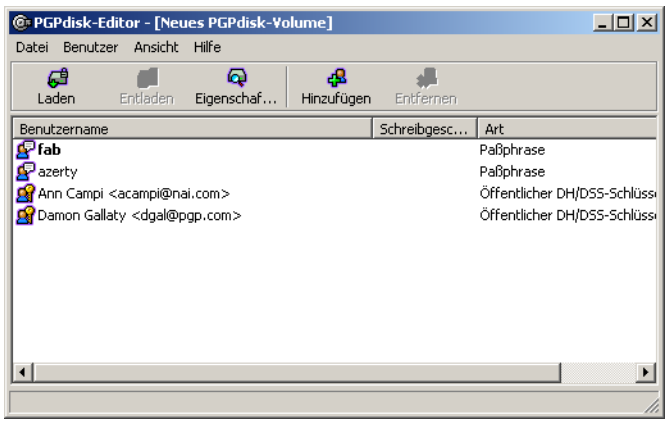


Abbildung 8-3. PGPdisk-Editor

Jedes PGPdisk-Volume verfügt über einen entsprechenden PGPdisk-Editor. Der PGPdisk-Editor zeigt die Liste der Benutzer an, die auf das Volume zugreifen dürfen, und gibt an, mit welcher Methode sich die Benutzer authentisieren. Die Authentisierung kann entweder mit einem öffentlichen Schlüssel oder mit einer Paßphrase erfolgen. Neben dem Namen des Administrators dieses Volumes wird das Symbol angezeigt. Den PGPdisk-Editor können Sie über den Windows-Explorer oder in PGPtray öffnen.

So öffnen Sie den PGPdisk-Editor über den Windows-Explorer:

1. Wählen Sie in der Verzeichnishierarchie im Windows-Explorer die verschlüsselte Volumedatei aus, die Sie ändern möchten.
2. Klicken Sie mit der rechten Maustaste auf den Namen der verschlüsselten Volumedatei. Daraufhin wird das Kontextmenü angezeigt.
3. Wählen Sie **PGP—>PGPdisk Bearbeiten**.

So öffnen Sie den PGPdisk-Editor in PGPtray:

1. Wählen Sie in PGPtray **PGPdisk—> Datenträger bearbeiten**.
2. Wählen Sie die verschlüsselte Volumedatei aus, die Sie bearbeiten möchten, und klicken Sie dann auf **Öffnen**.

PGPdisk verwenden

In diesem Abschnitt wird erläutert, wie Sie PGPdisk-Volumes erstellen, laden oder entladen können, und wie Eigenschaften festgelegt werden, mit denen der Inhalt eines Volumes geschützt ist, wenn es unter bestimmten Umständen entladen wird.

Neues PGPdisk-Volume erstellen

So erstellen Sie ein neues PGPdisk-Volume:

1. Klicken Sie auf **Start—>Programme—>PGP—>PGPdisk** (siehe Abbildung 8-1 auf Seite 146).
2. Auf dem Bildschirm wird der **PGPdisk-Erstellungsassistent** angezeigt. Lesen Sie die Einführung.
3. Klicken Sie auf **Weiter**. Es wird ein Dialogfeld angezeigt, in dem Sie den Speicherort und die Größe für das neue Volume festlegen können.
4. Klicken Sie auf **Durchsuchen**, um ein anderes Zielverzeichnis für Ihr PGPdisk-Volume auszuwählen, oder übernehmen Sie den Standardspeicherort.

Plattform:	Standardspeicherort:
Windows 95	C:\Eigene Dateien\
Windows 98	C:\Eigene Dateien\
Windows ME	C:\Eigene Dateien\
Windows NT	C:\WINNT\Profiles\{Name des aktuellen Benutzers}\Eigene Dateien\
Windows 2000	C:\Dokumente und Einstellungen\{Name des aktuellen Benutzers}\Eigene Dateien\

5. Geben Sie im Feld **Größe auswählen** an, wieviel Speicherplatz für das neue Volume reserviert werden soll. Verwenden Sie dabei nur ganze Zahlen ohne Dezimalstellen. Die im Feld angezeigte Größe können Sie mit Hilfe der Pfeile erhöhen bzw. verringern.

   Die Menge des auf dem ausgewählten Laufwerk zur Verfügung stehenden Speicherplatzes wird oberhalb des Feldes **Größe** angezeigt.

6. Wählen Sie aus der Größenliste eine der folgenden Maßeinheiten aus: **KB** (Kilobyte), **MB** (Megabyte) oder **GB** (Gigabyte).

   Das Volume muß mindestens 100 Kilobyte groß sein. Wie groß das PGPdisk-Volume maximal sein darf, hängt von Ihrer Windows-Version und von der Größe und dem Format Ihrer Festplatte ab.

7. Klicken Sie auf **Erweiterte Optionen**, um festzulegen, wo und wie Ihre PGPdisk geladen werden soll.

   Das Dialogfeld “Optionen” wird angezeigt (siehe Abbildung 8-4 auf Seite 151).

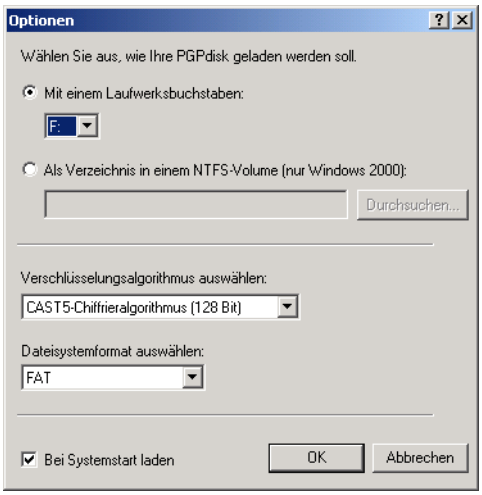


Abbildung 8-4. Dialogfeld “Optionen”

8. Legen Sie die gewünschten Optionen fest. Folgende Optionen stehen zur Wahl:

   - **Mit einem Laufwerksbuchstaben:** Wählen Sie den Buchstaben des Laufwerks aus, auf das Ihr neues PGPdisk-Volume geladen werden soll. In der Liste der Laufwerksbuchstaben sind alle verfügbaren Laufwerke aufgeführt. Ihr neues PGPdisk-Volume erscheint beim Laden an diesem Speicherort Ihrer Windows-Explorer-Ordnerhierarchie.

   - **Als Verzeichnis in einem NTFS-Volume:** Diese Option steht nur auf Windows 2000-Systemen zur Verfügung. Klicken Sie auf diese Option, wenn Sie Ihr neues PGPdisk-Volume als Verzeichnis auf einem NTFS-Volume laden möchten. Geben Sie den Pfad zu einem leeren Verzeichnis in dem zur Verfügung gestellten Speicherplatz ein, oder bewegen Sie sich zum gewünschten Speicherort.

Wenn Sie einen Pfad zu einem nicht vorhandenen Verzeichnis auf einem NTFS-Volume eingeben, werden Sie gefragt, ob ein Verzeichnis mit diesem Namen erstellt werden soll. Wählen Sie **Ja**, und geben Sie Ihre Paßphrase ein. Das Verzeichnis wird im Windows-Explorer auf dem ausgewählten NTFS-Volume angezeigt.

TIP: Klicken Sie mit der rechten Maustaste auf einen Laufwerksbuchstaben im Windows-Explorer, und wählen Sie **Eigenschaften**, um das Dateiformat für dieses Laufwerk herauszufinden.

- **Verschlüsselungsalgorithmus auswählen:** Wählen Sie den Verschlüsselungsalgorithmus aus, mit dem Ihre Daten geschützt werden sollen.
  - **CAST5-Chiffrieralgorithmus (128 Bit):** CAST ist eine 128-Bit-Blockverschlüsselung. Dieser zuverlässige, für militärische Zwecke geeignete Verschlüsselungsalgorithmus ist für seine Fähigkeit bekannt, unberechtigte Zugriffe wirksam zu verhindern.
  - **Twofish-Chiffrieralgorithmus (256 Bit):** Twofish ist ein neuer, von Bruce Schneier entwickelter symmetrischer 256-Bit-Blockverschlüsselungsalgorithmus. Er ist einer von fünf Algorithmen, die vom US-amerikanischen National Institute of Standards and Technology (NIST) für den Advanced Encryption Standard (AES) in Betracht gezogen werden, der den Data Encryption Standard (DES) ersetzt.
- **Dateisystemformat auswählen:** Legen Sie ein Dateisystemformat für das neue PGPdisk-Volume fest.
  - **FAT** (auf allen Windows-Plattformen verfügbar)
  - **NTFS** (nur auf Windows NT- und Windows 2000-Plattformen für PGPdisk-Volumes über 5 MB verfügbar)
  - **FAT32** (nur auf Windows 95-, Windows 98- Windows ME und Windows 2000- Plattformen für PGPdisk-Volumes über 260 MB verfügbar)
- **Bei Systemstart laden:** Aktivieren Sie diese Option, wenn die PGPdisk-Volumes beim Systemstart geladen werden sollen. Wenn Sie diese Option aktiviert haben, werden Sie beim Systemstart nach Ihrer PGPdisk-Paßphrase gefragt.

9. Klicken Sie auf **OK**. Das Dialogfeld “Optionen” wird geschlossen.
10. Klicken Sie auf **Weiter**.
11. Wählen Sie für Ihr neues PGPdisk-Volume eine Schutzmethode aus. Entscheiden Sie sich dazu für eine der folgenden Optionen:

    - **Öffentlicher Schlüssel:** Wenn Ihre PGPdisk mit einem öffentlichen Schlüssel geschützt werden soll, wird eine Liste der öffentlichen Schlüssel an Ihrem Schlüsselbund angezeigt. Markieren Sie den öffentlichen Schlüssel, mit dem Ihr neues PGPdisk-Volume geschützt werden soll.
    - **Paßphrase:** Wenn Ihre PGPdisk mit einer Paßphrase geschützt werden soll, müssen Sie auch einen Benutzernamen eingeben.

      Geben Sie die Folge von Zeichen oder Wörtern ein, die als Paßphrase für den Zugriff auf das neue Volume dienen soll (auch General-Paßphrase genannt). Drücken Sie die Tabulatortaste, um Ihre Eingabe zu bestätigen und zum nächsten Textfeld zu gelangen. Wiederholen Sie hier die Eingabe Ihrer Paßphrase. Die Paßphrase sollte aus mindestens acht Zeichen bestehen.

      Um zusätzliche Sicherheit zu gewährleisten, werden die Zeichen, die Sie für die Paßphrase eingeben, normalerweise nicht auf dem Bildschirm angezeigt. Wenn Sie jedoch sicher sind, daß Ihnen niemand zuschaut (direkt oder über das Netzwerk), und Sie die Zeichen Ihrer Paßphrase während der Eingabe sehen möchten, können Sie die Option **Eingabe verbergen** deaktivieren.

      HINWEIS: Ihre Sicherheit ist immer nur so gut wie Ihre Paßphrase. Weitere Informationen dazu finden Sie im Abschnitt “Einprägsame Paßphrasen erstellen” auf Seite 49.

      ---

12. Klicken Sie auf **Weiter**. Anhand der Verlaufsanzeige können Sie feststellen, inwieweit Ihr PGPdisk-Volume bereits initialisiert und formatiert ist.
13. Klicken Sie auf **Weiter**, um PGPdisk zu laden.
14. Klicken Sie auf **Fertig stellen**, damit Sie Ihr neues PGPdisk-Volume nutzen können.

    Ihr PGPdisk-Volume wird in einem Windows-Explorer-Fenster angezeigt.

Paßphrase für ein PGPdisk-Volume ändern

Alle Benutzer, die eine Paßphrase kennen, können diese auch ändern, aber der Administrator hat immer Zugang zum Inhalt des Volumes.

HINWEIS: Wenn Sie Ihr PGPdisk-Volume mit einem PGP-Schlüssel schützen möchten, müssen Sie die Paßphrase für Ihren privaten Schlüssel in PGPkeys ändern. Im PGPdisk-Editor ist dies nicht möglich.

So ändern Sie Ihre Paßphrase:

1. Stellen Sie sicher, daß das PGPdisk-Volume nicht geladen ist. Wenn das PGPdisk-Volume geladen ist, ist es nicht möglich, die Paßphrase zu ändern.
2. Öffnen Sie den PGPdisk-Editor für das Volume, das Sie bearbeiten möchten, und wählen Sie dann den Benutzernamen aus, der zu der zu ändernden Paßphrase gehört.
3. Wählen Sie im Menü **Benutzer** den Befehl **Paßphrase ändern**.

   Das Dialogfeld “Paßphrase eingeben” wird angezeigt.

4. Geben Sie Ihre Paßphrase ein, und klicken Sie auf **OK**.

   Daraufhin wird das Fenster **Neue Paßphrase eingeben** angezeigt.

5. Geben Sie die Folge von Zeichen oder Wörtern ein, die als Paßphrase für den Zugriff auf das neue Volume dienen soll (auch Administrator-Paßphrase genannt). Drücken Sie die Tabulatortaste, um Ihre Eingabe zu bestätigen und zum nächsten Textfeld zu gelangen. Wiederholen Sie hier die Eingabe Ihrer Paßphrase. Die Paßphrase sollte aus mindestens acht Zeichen bestehen.
6. Klicken Sie auf **OK**.

   Das Dialogfeld “Neue Paßphrase eingeben” wird geschlossen. Die Paßphrase ist damit geändert.

Alternative Benutzer zu einem PGPdisk-Volume hinzufügen

Der PGPdisk-Administrator kann festlegen, daß die PGPdisk für alternative Benutzer zugänglich ist. Der Zugriff auf das Volume kann entweder über die eindeutige Paßphrase oder aber über einen privaten Schlüssel erfolgen. Alternative Benutzer können nur von der Person hinzugefügt werden, die die Administrator-Paßphrase kennt.

Sie haben auch die Möglichkeit, dem Volume einen schreibgeschützten Status zuzuweisen. Alternative Benutzer können die Dateien dann zwar lesen, Änderungen daran können sie aber nicht vornehmen.

So fügen Sie alternative Benutzer hinzu:

1. Stellen Sie sicher, daß das PGPdisk-Volume zur Zeit nicht geladen ist. Wenn das PGPdisk-Volume geladen ist, ist es nicht möglich, alternative Benutzer hinzuzufügen.
2. Öffnen Sie den PGPdisk-Editor für das Volume, das Sie bearbeiten möchten, und wählen Sie dann den Befehl **Hinzufügen** aus dem Menü **Benutzer**.

   Daraufhin wird das Dialogfeld “Paßphrase eingeben” angezeigt, in dem Sie zur Eingabe der Administrator-Paßphrase aufgefordert werden.
3. Geben Sie die Administrator-Paßphrase ein, und klicken Sie auf **OK**.

   Daraufhin wird der “PGPdisk-Assistent für die Benutzererstellung” angezeigt. Lesen Sie die Einführung.
4. Klicken Sie auf **Weiter**.

5. Wählen Sie für den neuen Benutzer eine Schutzmethode aus. Folgende Optionen stehen zur Wahl:

   - **Öffentlicher Schlüssel:** Wenn Ihre PGPdisk mit einem öffentlichen Schlüssel geschützt werden soll, wird eine Liste der öffentlichen Schlüssel an Ihrem Schlüsselbund angezeigt. Markieren Sie den öffentlichen Schlüssel des alternativen Benutzers.

     TIP: Die Verwendung eines öffentlichen Schlüssels stellt die sicherste Schutzmethode beim Hinzufügen alternativer Benutzer zu einem PGPdisk-Volume dar. Dafür gibt es folgende Gründe: (1) Das Austauschen der Paßphrase mit dem alternativen Benutzer, das je nach Ihrer Methode mitgehört oder belauscht werden kann, ist nicht notwendig. (2) Der alternative Benutzer muß sich keine weitere Paßphrase merken, die er unter Umständen später vergißt. (3) Das Verwalten einer Liste alternativer Benutzer ist einfacher, wenn jeder zum Zugriff auf das Volume seinen eigenen privaten Schlüssel verwendet.

   - **Paßphrase:** Wenn Ihre PGPdisk mit einer Paßphrase geschützt werden soll, müssen Sie auch den Namen des alternativen Benutzers eingeben.

     Geben Sie die Folge von Zeichen oder Wörtern ein, die als Paßphrase für den Zugriff auf das neue Volume dienen soll. Drücken Sie die Tabulatortaste, um Ihre Eingabe zu bestätigen und zum nächsten Textfeld zu gelangen. Wiederholen Sie hier die Eingabe Ihrer Paßphrase. Die Paßphrase sollte aus mindestens acht Zeichen bestehen.

     Um zusätzliche Sicherheit zu gewährleisten, werden die Zeichen, die Sie für die Paßphrase eingeben, normalerweise nicht auf dem Bildschirm angezeigt. Wenn Sie jedoch sicher sind, daß Ihnen niemand zuschaut (direkt oder über das Netzwerk), und Sie die Zeichen Ihrer Paßphrase während der Eingabe sehen möchten, können Sie die Option **Eingabe verbergen** deaktivieren.

     HINWEIS: Ihre Sicherheit ist immer nur so gut wie Ihre Paßphrase. Weitere Informationen dazu finden Sie im Abschnitt “Einprägsame Paßphrasen erstellen” auf Seite 49.

     ---

6. Klicken Sie auf **Weiter**. Anhand der Verlaufsanzeige können Sie feststellen, inwieweit Ihr PGPdisk-Volume bereits initialisiert und formatiert ist.

7. Klicken Sie auf **Fertig stellen**. Der alternative Benutzer ist damit hinzugefügt.

   Die von Ihnen hinzugefügten alternativen Benutzer können Sie jederzeit durch Wählen des Befehls **Entfernen** im Menü **Benutzer** wieder entfernen. Weitere Informationen finden Sie im Abschnitt “Alternative Benutzer von einem PGPdisk-Volume entfernen” auf Seite 157.

So weisen Sie den schreibgeschützten Status zu:

1. Öffnen Sie den PGPdisk-Editor für das Volume, das Sie bearbeiten möchten, und wählen Sie dann den Benutzernamen.
2. Wählen Sie **Auf Schreibschutz umschalten** im Menü **Benutzer**.

   Daraufhin wird das Dialogfeld “Paßphrase eingeben” angezeigt, in dem Sie zur Eingabe der Administrator-Paßphrase aufgefordert werden.
3. Geben Sie die Administrator-Paßphrase ein, und klicken Sie auf **OK**.

   Neben dem Benutzernamen in der Spalte **Schreibgeschützt** wird ein roter Punkt ( ) angezeigt.

   Wenn Sie einem Benutzer den Status “Schreibgeschützt” zugewiesen haben, können Sie diese Einschränkung auch wieder aufheben, indem Sie die oben genannten Schritte erneut ausführen.

Alternative Benutzer von einem PGPdisk-Volume entfernen

Der Vorgang zum Entfernen eines alternativen Benutzers ist dem zum Hinzufügen eines alternativen Benutzers oder Ändern einer Paßphrase ähnlich.

So entfernen Sie alternative Benutzer:

1. Stellen Sie sicher, daß das PGPdisk-Volume momentan nicht geladen ist. Wenn das PGPdisk-Volume geladen ist, ist es nicht möglich, alternative Benutzer zu entfernen.
2. Öffnen Sie den PGPdisk-Editor für das Volume, das Sie bearbeiten möchten, und wählen Sie dann den Benutzernamen aus, der aus der Liste entfernt werden soll.

3. Wählen Sie den Befehl **Entfernen** aus dem Menü **Benutzer**.

   Das Dialogfeld “Paßphrase eingeben” wird angezeigt, in dem Sie aufgefordert werden, die Administrator-Paßphrase bzw. die Paßphrase für den zu entfernenden Benutzer einzugeben.

4. Geben Sie die Paßphrase ein, und klicken Sie auf **OK**. Der Benutzer ist damit entfernt.

PGPdisk-Volume laden

Beim Erstellen eines neuen Volumes wird dieses durch das PGPdisk-Programm automatisch geladen, so daß Sie es sofort zum Speichern Ihrer Dateien verwenden können. Wenn Sie den Inhalt des Volumes sichern möchten, müssen Sie das Volume entladen (weitere Informationen dazu finden Sie unter “PGPdisk-Volume entladen” auf Seite 159). Nachdem ein Volume entladen wurde, ist der Inhalt des Volumes in einer verschlüsselten Datei gespeichert und erst wieder zugänglich, wenn das Volume wieder geladen wird.

Zum Laden eines Volumes gibt es mehrere Möglichkeiten:

- Klicken Sie mit der rechten Maustaste im Windows-Explorer auf die PGPdisk-Datei, und wählen Sie **PGP—>PGPdisk laden** (siehe Abbildung 8-2 auf Seite 147).
- Wählen Sie in PGPtray **PGPdisk—> Datenträger laden**.
- Klicken Sie im PGPdisk-Editor auf die Schaltfläche **Laden**, bzw. wählen Sie den Befehl **Laden** im Menü **Datei**.

Daraufhin wird das geladene PGPdisk-Volume in einem Windows-Explorer-Fenster als leeres Laufwerk angezeigt.

Geladenes PGPdisk-Volume verwenden

Sie können Dateien und Ordner auf einem PGPdisk-Volume wie auf jedem anderen Volume erstellen, kopieren, verschieben und löschen. Analog kann jeder andere Benutzer, der (entweder auf demselben Rechner oder evtl. über das Netzwerk) über Zugriff auf das Volume verfügt, ebenfalls auf die im Volume gespeicherten Daten zugreifen. Erst wenn Sie das Volume entladen, kann auf die Daten in der dem Volume zugeordneten verschlüsselten Datei nicht mehr zugegriffen werden.

WARNUNG: Obwohl die verschlüsselten, den einzelnen Volumes zugeordneten Dateien vor mißbräuchlichem Zugriff geschützt sind, können sie gelöscht werden. Wenn eine unbefugte Person auf Ihre Daten zugreifen kann, ist es möglich, daß sie die verschlüsselte Datei löscht, die die Grundlage für das Volume bildet. Es wird daher empfohlen, eine Sicherungskopie der verschlüsselten Datei zu erstellen.

PGPdisk-Volume entladen

Wenn Sie auf ein bestimmtes Volume nicht mehr zugreifen und dessen Inhalt sperren möchten, müssen Sie das Volume entladen.

WARNUNG: Beim Entladen von PGPdisk-Volumes, bei denen noch Dateien geöffnet sind, können Daten verlorengehen. Wenn Sie die Optionen **Erzwungene Entladung von PGPdisks bei geöffneten Dateien zulassen** und **Vor erzwungener Entladung einer PGPdisk nicht anfragen** auf der Registerkarte **PGP-Optionen** aktiviert haben, wird keine Warnung angezeigt, bevor ein Volume mit geöffneten Dateien entladen wird. Sie laufen dann Gefahr, die in dem Volume gespeicherten Daten zu verlieren. Weitere Informationen zum Festlegen von PGP-Optionen finden Sie im Abschnitt “Optionen für die persönliche Firewall festlegen” auf Seite 263.

Zum Entladen eines Volumes gibt es mehrere Möglichkeiten:

- Klicken Sie mit der rechten Maustaste im Windows-Explorer auf die PGPdisk-Datei, und wählen Sie **PGP—>PGPdisk Entladen** (siehe Abbildung 8-2 auf Seite 147).
- Klicken Sie im PGPdisk-Editor auf die Schaltfläche **Entladen**, bzw. wählen Sie den Befehl **Entladen** aus dem Menü **Datei**.
- Wählen Sie in PGPtray **PGPdisk—> Alle Datenträger entladen**.
- Erstellen Sie zum Entladen aller PGPdisks in einem Schritt einen entsprechenden Tastaturbefehl (Hotkey). Genaue Anweisungen dazu, wie Sie Tastaturbefehle erstellen können, finden Sie im Abschnitt “HotKey-Optionen festlegen” auf Seite 253.
- (nur in Windows 2000 und Windows NT) **Drücken Sie die Tastenkombination Strg+Alt+Entf, und wählen Sie die Option PGPdisks entladen**.

Wenn ein Volume entladen ist, wird sein Inhalt in der verschlüsselten, dem Volume zugeordneten Datei gesperrt. Der Inhalt des Volumes wird in der verschlüsselten Datei gespeichert, und ist erst wieder zugänglich, wenn das Volume geladen wird. Es ist möglicherweise hilfreich, PGPdisk-Volumes als Fenster anzuzeigen, in dem die Daten in der verschlüsselten Datei angezeigt werden können. Der Inhalt einer PGPdisk-Datei ist erst verfügbar, wenn ein Benutzer eine gültige Paßphrase kennt und die Datei als Volume lädt.

Eigenschaften für ein PGPdisk-Volume festlegen

Über die Schaltfläche **Eigenschaften** im PGPdisk-Editor können Sie herausfinden, welche Ladeoptionen gelten und welcher Verschlüsselungsalgorithmus für das betreffende Volume verwendet wurde. Außerdem können Sie über diese Schaltfläche das Volume neu verschlüsseln. Wenn Sie für alle PGPdisk-Volumes gültige PGP-Optionen festlegen möchten, finden Sie Informationen dazu im Abschnitt “Optionen für die persönliche Firewall festlegen” auf Seite 263.

So legen Sie die Eigenschaften fest:

1. Öffnen Sie den PGPdisk-Editor für das Volume, das Sie bearbeiten möchten, und klicken Sie dann auf **Eigenschaften**, bzw. wählen Sie den Befehl **Eigenschaften** aus dem Menü **Datei**.

   Das Dialogfeld “Eigenschaften” wird angezeigt.

2. Wählen Sie die gewünschten Optionen, indem Sie auf die entsprechenden Kontrollkästchen klicken.

   - **Neu verschlüsseln**: Wenn diese Option aktiviert ist, können Sie den Verschlüsselungsalgorithmus des PGPdisk-Volume ändern bzw. Ihre PGPdisk erneut mit demselben Verschlüsselungsalgorithmus verschlüsseln, wobei aber der zugrundeliegende Verschlüsselungsschlüssel geändert wird. Dies kann erforderlich werden, wenn Sie das Gefühl haben, daß die Sicherheit Ihrer PGPdisk gefährdet ist, oder wenn Sie einen Benutzer von der PGPdisk entfernt haben und ganz sicher gehen möchten, daß dieser Benutzer nicht mehr darauf zugreifen kann.

WICHTIG: Erfahrene Benutzer sind unter Umständen in der Lage, im Arbeitsspeicher ihrer Computer nach dem den PGPdisks zugrundeliegenden Verschlüsselungsschlüssel zu suchen und diesen zu speichern. Selbst wenn sie dann als Benutzer von der Benutzerliste entfernt worden sind, können sie weiterhin auf die PGPdisk zugreifen. Beim Neuverschlüsseln ändert sich der zugrundeliegende Verschlüsselungsschlüssel, wodurch solche Benutzer dann am Zugriff gehindert werden.

- **Bei Systemstart laden:** Aktivieren Sie diese Option, wenn das PGPdisk-Volume beim Systemstart geladen werden soll. Wenn Sie diese Option aktiviert haben, werden Sie beim Systemstart nach Ihrer PGPdisk-Paßphrase gefragt.
- **Globale Optionen für das automatische Laden außer Kraft setzen:** Wenn diese Option aktiviert ist, wird die globale Option für das automatische Entladen, die für das ausgewählte PGPdisk-Volume auf der Registerkarte **PGP-Optionen** festgelegt wurde, außer Kraft gesetzt. Genauere Informationen zum Festlegen von PGP-Optionen finden Sie im Abschnitt “Optionen für die persönliche Firewall festlegen” auf Seite 263.

HINWEIS: Die Option für das automatische Entladen, die Sie auf der Registerkarte **PGP-Optionen** festgelegt haben, trifft für alle geladenen PGPdisk-Volumes zu. Wenn ein Volume zu einem anderen Zeitpunkt automatisch entladen werden soll, als Sie mit der Option für das automatische Entladen festgelegt haben, müssen Sie diese außer Kraft setzen.

Die dazu nötige Option **Automatische Entladung nach [15] Minuten Inaktivität** ist verfügbar, wenn Sie sich dafür entschieden haben, die globale Option für das automatische Entladen außer Kraft zu setzen. PGP ist dadurch in der Lage, automatisch das PGPdisk-Volume zu entladen, wenn auf Ihrem Computer während des in Minuten angegebenen Zeitraums keine Aktivitäten stattfinden. Als Inaktivitätszeitraum kann jeder Wert von 1 bis 999 Minuten festgelegt werden.

PGPdisk-Volumes verwalten

In diesem Abschnitt wird beschrieben, wie Sie festlegen können, daß PGPdisk-Volumes beim Systemstart automatisch geladen werden, wie Sie Sicherungskopien von Daten erstellen und die Daten auf diesen Volumes mit anderen Benutzern austauschen können und wie Sie Ihr PGPdisk-Volume neu verschlüsseln können.

PGPdisk-Volumes automatisch laden

Sie können PGPdisk-Volumes beim Systemstart automatisch laden lassen.

Daß ein Volume automatisch geladen werden soll, kann auf verschiedene Art und Weise festgelegt werden:

- Aktivieren Sie beim Erstellen Ihres PGPdisk-Volumes die Option **Bei Systemstart laden** im Dialogfeld “Optionen”. Weitere Informationen dazu finden Sie im Abschnitt “Neues PGPdisk-Volume erstellen” auf Seite 150.
- Aktivieren Sie die Option **Bei Systemstart laden** im Dialogfeld “Eigenschaften” des Volumes, das automatisch geladen werden soll. Weitere Informationen dazu finden Sie im Abschnitt “Eigenschaften für ein PGPdisk-Volume festlegen” auf Seite 160.
- Erstellen Sie eine Verknüpfung für jede PGPdisk-Datei, die beim Starten Ihres Computers automatisch geladen werden soll. Weitere Informationen dazu finden Sie weiter unten.

So können Sie festlegen, daß PGPdisk-Volumes automatisch geladen werden:

1. Erstellen Sie eine Verknüpfung für jede PGPdisk-Datei, die beim Starten Ihres Computers geladen werden soll.
2. Speichern Sie die Verknüpfungen im Ordner **WINNT\Profiles\{Name des aktuellen Benutzers}\Startmenü\Programme\Autostart**.

   Wenn sich die Verknüpfungen in diesem Ordner befinden, werden die PGPdisk-Volumes bei jedem Starten Ihres Computers geladen. Sie werden beim Laden der einzelnen PGPdisk-Volumes aufgefordert, die entsprechende Paßphrase einzugeben.

PGPdisk-Dateien auf einem entfernten Server laden

Sie können PGPdisk-Volumes auf allen Arten von Servern (Windows oder UNIX) ablegen. Diese Volumes können dann von allen Benutzern geladen werden, die über einen Computer mit Windows verfügen.

HINWEIS: Der erste Benutzer, der das Volume lokal lädt, verfügt über Lese- und Schreibzugriff auf das Volume. Danach kann kein anderer auf das Volume zugreifen. Wenn Sie wünschen, daß auch andere Benutzer auf Dateien innerhalb dieses Volumes zugreifen können, müssen Sie das Volume im schreibgeschützten Modus laden (nur bei den Dateisystemen FAT und FAT32). *Alle* Benutzer des Volumes können das Volume dann lesen, nicht aber die Daten im Volume ändern.

Wenn das Volume auf einem Windows-Server gespeichert ist, können Sie das Volume auch auf dem entfernten Server laden und damit die gemeinsame Nutzung des geladenen Volumes zulassen. Bei diesem Vorgang ist allerdings die Sicherheit für die Dateien im Volume nicht gewährleistet.

Sicherungskopien von PGPdisk-Volumes erstellen

Es wird empfohlen, Sicherungskopien des Inhalts Ihrer PGPdisk-Volumes zu erstellen, um Ihre Daten bei Systemausfällen und Festplattenfehlern zu schützen. Obwohl es möglich ist, eine Sicherungskopie des Inhalts eines geladenen PGPdisk-Volumes wie bei jedem anderen Volume zu erstellen, können wir dies nicht empfehlen, da der Inhalt nicht verschlüsselt wird und somit jedem zugänglich ist, der die Sicherungskopie wiederherstellen kann. Statt den Inhalt eines geladenen PGPdisk-Volumes zu sichern, sollten Sie eine Sicherungskopie des verschlüsselten PGPdisk-Volumes erstellen.

So erstellen Sie Sicherungskopien von PGPdisk-Volumes:

1. Entladen Sie das PGPdisk-Volume. Weitere Informationen zum Entladen von PGPdisk-Volumes finden Sie im Abschnitt “PGPdisk-Volume entladen” auf Seite 159.

2. Kopieren Sie die entladene, verschlüsselte Datei auf eine Diskette, ein Band oder einen Wechseldatenträger analog zur Vorgehensweise bei einer normalen Datei. Selbst wenn eine unbefugte Person Zugriff auf die Sicherungskopie hat, kann sie deren Inhalt nicht entschlüsseln.

Beim Erstellen von Sicherungskopien der verschlüsselten Dateien müssen Sie an folgendes denken:

- PGPdisk ist ein Produkt für sicherheitsbewußte Personen und Organisationen. Wenn die Sicherungskopie der verschlüsselten Dateien auf einem Netzlaufwerk abgelegt wird, kann eine schwache Paßphrase von unbefugten Benutzern durch Probieren leicht herausgefunden werden. Wir empfehlen Ihnen, Sicherungskopien nur auf Geräten zu erstellen, auf die Sie physischen Zugang haben. Durch eine längere, komplizierte Paßphrase wird das Sicherheitsrisiko weiter gemindert. Siehe dazu “Einprägsame Paßphrasen erstellen” auf Seite 49.
- Wenn Ihr Computer an ein Netzwerk angeschlossen ist, müssen Sie dafür sorgen, daß die im Netzwerk eingesetzten Netzwerksicherungssysteme keine Sicherungskopien der geladenen Volumes erstellen. Möglicherweise müssen Sie dies mit Ihrem System-Administrator absprechen. Unter Umständen spielt es keine Rolle, ob Sicherungskopien von Ihren verschlüsselten Dateien erstellt werden, da diese Informationen sicher sind. Auf keinen Fall dürfen jedoch Sicherungskopien des Inhalts Ihrer geladenen Volumes erstellt werden, da dadurch diese Informationen nicht mehr verschlüsselt sind.

PGPdisk-Volumes austauschen

Sie können PGPdisk-Volumes mit Kollegen austauschen, die über ein eigenes PGPdisk-Programm verfügen, indem Sie ihnen eine Kopie der verschlüsselten Datei mit den dem Volume zugeordneten Daten senden. Zum Austauschen von PGPdisk-Volumes gibt es folgende Möglichkeiten:

- als E-Mail-Anhänge
- auf Disketten oder Magnetbändern
- über ein Netzwerk

TIP: Die Verwendung eines öffentlichen Schlüssels stellt die sicherste Schutzmethode beim Hinzufügen alternativer Benutzer zu einem PGPdisk-Volume dar. Dafür gibt es folgende Gründe: (1) Das Austauschen der Paßphrase mit dem alternativen Benutzer, das je nach Ihrer Methode mitgehört oder belauscht werden kann, ist nicht notwendig. (2) Der alternative Benutzer muß sich keine weitere Paßphrase merken, die er unter Umständen später vergißt. (3) Das Verwalten einer Liste alternativer Benutzer ist einfacher, wenn jeder zum Zugriff auf das Volume seinen eigenen privaten Schlüssel verwendet. Je mehr Sicherheitsvorkehrungen Sie treffen, desto sicherer können Sie sein, daß Ihre vertraulichen Informationen auch geheim bleiben.

Wenn die Zielperson eine Kopie der verschlüsselten Datei erhalten hat, muß das Volume nur noch mit der entsprechenden Paßphrase bzw. mit dem privaten Schlüssel (wenn die Verschlüsselung des Volumes auf dem öffentlichen Schlüssel der Zielperson basiert) geladen werden. Außerdem benötigen Sie PGPdisk. Weitere Informationen zum Laden eines PGPdisk-Volumes finden Sie im Abschnitt “PGPdisk-Volume laden” auf Seite 158.

Größe eines PGPdisk-Volumes ändern

Die Größe eines bereits erstellten PGPdisk-Volumes kann zwar nicht geändert werden, dafür können Sie aber ein größeres oder kleineres Volume erstellen und dann den Inhalt des alten Volumes in das neue Volume kopieren.

So ändern Sie die Größe eines PGPdisk-Volumes:

1. Erstellen Sie ein neues PGPdisk-Volume, und geben Sie die gewünschte Größe an. Weitere Informationen zum Erstellen eines neuen Volumes finden Sie im Abschnitt “Neues PGPdisk-Volume erstellen” auf Seite 150.
2. Kopieren Sie den Inhalt des vorhandenen geladenen PGPdisk-Volumes in das neu erstellte Volume.
3. Entladen Sie das alte PGPdisk-Volume, und löschen Sie dann die dem Volume zugeordnete verschlüsselte Datei, um den Speicherplatz wieder freizugeben.

PGPdisk-Volumes neu verschlüsseln

Mit PGP sind Sie in der Lage, alle auf einer PGPdisk gespeicherten Daten neu zu verschlüsseln. Auf diese Weise können Sie den Schutz Ihrer Daten in Umgebungen erhöhen, die ein höheres Maß an Sicherheit erfordern. Durch Neuverschlüsseln können Sie den Verschlüsselungsalgorithmus ändern, mit dem das Volume geschützt wurde, bzw. Ihre PGPdisk erneut mit demselben Verschlüsselungsalgorithmus verschlüsseln, wobei aber der zugrundeliegende Verschlüsselungsschlüssel geändert wird.

WICHTIG: Ein erfahrener Benutzer ist unter Umständen in der Lage, im Arbeitsspeicher seines Computers nach dem der PGPdisk zugrundeliegenden Verschlüsselungsschlüssel zu suchen und diesen zu speichern, um auch dann noch auf die PGPdisk zugreifen zu können, wenn er bereits von der Benutzerliste entfernt worden ist. Beim Neuverschlüsseln ändert sich der zugrundeliegende Verschlüsselungsschlüssel, wodurch solche Benutzer dann am Zugriff gehindert werden.

So verschlüsseln Sie ein PGPdisk-Volume neu:

1. Öffnen Sie den PGPdisk-Editor für das Volume, das Sie bearbeiten möchten, und klicken Sie dann auf **Eigenschaften**, bzw. wählen Sie den Befehl **Eigenschaften** aus dem Menü **Datei**.

   Das Dialogfeld “Eigenschaften” wird angezeigt.

2. Klicken Sie auf die Schaltfläche **Neu verschlüsseln**.

3. Geben Sie Ihre Paßphrase für das Volume ein.

   Daraufhin wird der “PGPdisk-Assistent für Neuverschlüsselung” angezeigt.

4. Lesen Sie die einleitenden Informationen, und klicken Sie dann auf **Weiter**.

   Daraufhin wird ein Dialogfeld mit dem aktuellen Verschlüsselungsalgorithmus, mit dem Ihr PGPdisk-Volume geschützt ist, und dem neuen Verschlüsselungsalgorithmus angezeigt.

   Wenn Ihre PGPdisk beispielsweise derzeit mit CAST verschlüsselt ist, wird in der Liste “Neuer Algorithmus” “Twofish-Chiffrieralgorithus (256 Bit)” angezeigt und umgekehrt.

5. Legen Sie eine der folgenden Optionen fest:

   - Aktivieren Sie die Option **Mit demselben Algorithmus verschlüsseln**, wenn die PGPdisk unter Verwendung des aktuellen Algorithmus neu verschlüsselt werden soll, und klicken Sie dann auf **Weiter**.

     oder

   - Klicken Sie auf **Weiter**, wenn die PGPdisk mit dem in der Dropdown-Liste **Neuer Algorithmus** angezeigten Algorithmus neu verschlüsselt werden soll.

   Die PGPdisk wird mit dem von Ihnen ausgewählten Verschlüsselungsalgorithmus neu verschlüsselt.

6. Wenn als aktueller Status **Fertig** angezeigt wird, klicken Sie auf **Weiter**.

7. Klicken Sie auf **Fertig stellen**, um den Neuverschlüsselungsprozeß abzuschließen.

Technische Daten und Sicherheitsvorkehrungen

In diesem Abschnitt werden Aspekte zur Verschlüsselung und zu Sicherheitsvorkehrungen besprochen sowie Hinweise für Benutzer und technische Informationen zu PGPdisk gegeben.

Überblick über PGPdisk-Volumes

PGPdisk-Volumes unterstützen das Strukturieren Ihrer Arbeit, das Auseinanderhalten von Dateien mit ähnlichen Namen und die getrennte Aufbewahrung von verschiedenen Versionen eines Dokuments oder Programms.

Obwohl die von Ihnen mit der PGPdisk-Funktion erstellten Volumes wie normale, Ihnen bereits bekannte Volumes funktionieren, werden die Daten in einer großen verschlüsselten Datei gespeichert. Nur wenn Sie die Datei laden, wird der Inhalt in Form eines Volumes dargestellt. Ihre gesamten Daten bleiben in der verschlüsselten Datei gesichert und werden nur entschlüsselt, wenn Sie auf eine der Dateien zugreifen. Wenn die Daten für ein Volume auf diese Weise gespeichert werden, können PGPdisk-Volumes problemlos mit anderen ausgetauscht oder bearbeitet werden. Allerdings können Daten auch leichter verlorengehen, wenn die Datei versehentlich gelöscht wird. Es empfiehlt sich, eine Sicherungskopie dieser verschlüsselten Dateien zu erstellen, damit die Daten wiederhergestellt werden können, falls die Originaldatei beschädigt wird.

Sie können die verschlüsselten Dateien selbst zwar nicht komprimieren, um deren Größe zu verringern, jedoch können Sie die einzelnen Dateien im geladenen Volume komprimieren und dadurch eine größere Zahl verschlüsselter Daten im Volume speichern. Außerdem können Sie ein geschütztes PGPdisk-Volume in einem anderen speichern und so verschiedene Volumes ineinander einbetten, um den Grad der Sicherheit zu erhöhen.

Die PGPdisk-Verschlüsselungsalgorithmen

Bei der Verschlüsselung werden Ihre Daten mit Hilfe einer mathematischen Formel so durcheinandergewirbelt, daß sie für andere vollkommen wertlos sind. Durch Anwendung des richtigen mathematischen Schlüssel lassen sich die Daten wieder entschlüsseln. Bei der PGPdisk-Verschlüsselungsformel kommen für einen Teil des Verschlüsselungsprozesses Zufallsdaten zum Einsatz. Einige dieser Zufallsdaten werden auf der Grundlage der Bewegung Ihrer Maus während der Verschlüsselung generiert, während andere dagegen direkt auf Ihrer Paßphrase beruhen.

In PGPdisk stehen Ihnen zwei leistungsstarke Algorithmusoptionen zum Schutz Ihrer PGPdisk-Volumes zur Verfügung: CAST und Twofish.

CAST gilt aufgrund seiner Schnelligkeit und hohen Entschlüsselungssicherheit als ausgezeichnetes Blockverschlüsselungsverfahren. Sein Name basiert auf den Initialen von Carlisle Adams und Stafford Tavares von der Firma Northern Telecom (Nortel), die das Verfahren entwickelt haben und einen guten Ruf auf diesem Gebiet genießen. Nortel hat CAST zum Patent angemeldet, sich gleichzeitig aber verpflichtet, CAST lizenzgebührenfrei allgemein zugänglich zu machen. Mit CAST steht ein außergewöhnlich gut entwickeltes Verfahren zur Verfügung, dem ein sehr formeller Ansatz zu Grunde liegt. Eine Reihe von formell beweisbaren Aussagen machen es sehr glaubhaft, daß eine Entschlüsselung seines 128-Bit-Schlüssels möglicherweise nur unter völliger Ausschöpfung des Schlüssels möglich ist. CAST kennt keine schwachen Schlüssel. Vieles spricht dafür, daß CAST sowohl gegen die lineare als auch gegen die differentielle Kryptoanalyse immun ist – die beiden stärksten Formen der Kryptoanalyse, die in der veröffentlichten Literatur bisher beschrieben wurden. Beide Formen haben beim “Einbrechen” in den Data Encryption Standard (DES) eine Rolle gespielt.

Twofish ist ein von Bruce Schneier entwickelter symmetrischer 256-Bit-Blockverschlüsselungsalgorithmus, der bereits auf große Resonanz gestoßen ist. Er ist einer von fünf Algorithmen, die vom US-amerikanischen National Institute of Standards and Technology (NIST) für den neuen Advanced Encryption Standard (AES) in Betracht gezogen werden. AES ersetzt den Data Encryption Standard (DES).

Besondere Sicherheitsvorkehrungen von PGPdisk

PGPdisk trifft spezielle Vorkehrungen, um Sicherheitsprobleme zu vermeiden, was bei anderen Programmen möglicherweise nicht der Fall ist. Dazu gehören folgende Funktionen:

Löschen der Paßphrase

Wenn Sie eine Paßphrase eingeben, wird sie von PGPdisk nur für kurze Zeit verwendet und dann aus dem Speicher gelöscht. PGPdisk verhindert auch, daß Kopien von der Paßphrase erstellt werden. Folglich verbleibt Ihre Paßphrase in der Regel nur einen Bruchteil einer Sekunde im Speicher. Diese Funktion ist von besonderer Bedeutung, denn bliebe die Paßphrase im Speicher, könnte jemand dort nach ihr suchen, wenn Ihr Computer unbeaufsichtigt ist. Sie würden davon nichts merken, doch diejenige Person hätte dann vollen Zugriff auf alle PGPdisk-Volumes, die von dieser Paßphrase geschützt werden.

Schutz des virtuellen Speichers

Ihre Paßphrase oder andere Schlüssel könnten auf Festplatte geschrieben werden, wenn das virtuelle Speichersystem Speicherdaten auf die Festplatte auslagert. PGPdisk sorgt dafür, daß Paßphrasen und Schlüssel nie auf Festplatte geschrieben werden. Diese Funktion ist besonders wichtig, da jemand die virtuelle Speicherdatei nach Paßphrasen durchsuchen könnte.

Schutz vor statischen Ionenmigrationen im Arbeitsspeicher

Wenn Sie eine PGPdisk laden, wird Ihre Paßphrase in einen Schlüssel umgewandelt. Mit Hilfe dieses Schlüssels werden die Daten auf Ihrem PGPdisk-Volume ver- und entschlüsselt. Im Unterschied zur Paßphrase, die sofort aus dem Arbeitsspeicher gelöscht wird, verbleibt der Schlüssel (aus dem Ihre Paßphrase nicht abgeleitet werden kann) im Arbeitsspeicher, während das Volume geladen wird. Dieser Schlüssel wird im virtuellen Speicher geschützt. Wenn aber ein Teil des Arbeitsspeichers dieselben Daten über äußerst lange Zeiträume hinweg speichert, ohne heruntergefahren oder zurückgesetzt zu werden, neigt dieser Arbeitsspeicher zum Beibehalten eines statischen Ladezustands, der von Angreifern gelesen werden könnte. Wenn Ihre PGPdisk für lange Zeit geladen ist, ist es nach gewisser Zeit möglich, daß “Spuren” Ihres Schlüssels im Arbeitsspeicher verbleiben und dort aufgespürt werden können. Es gibt Geräte, mit denen der Schlüssel wiederhergestellt werden kann. Solche Geräte bekommen Sie zwar nicht gerade im Elektronikladen um die Ecke, aber es gibt durchaus größere Institutionen oder Behörden, wo so etwas vorhanden sein kann.

PGPdisk schützt Sie davor, indem im RAM zwei Kopien des Schlüssels aufbewahrt werden – eine normale Kopie und eine bitinvertierte Kopie –, die zudem noch alle paar Sekunden invertiert werden.

Andere Sicherheitsvorkehrungen

In der Regel hängt der Schutz Ihrer Daten von den durch Sie getroffenen Vorkehrungen ab, denn kein Verschlüsselungsprogramm kann Ihre Daten schützen, wenn unzureichende Vorsichtsmaßnahmen getroffen werden. Wenn beispielsweise Ihr Computer eingeschaltet ist und Sie vertrauliche Dateien geöffnet haben und Ihren Arbeitsplatz verlassen, kann jeder auf diese Informationen zugreifen und sogar den Schlüssel für den Zugriff auf die Daten erhalten. Beachten Sie daher zum optimalen Schutz folgende Tips:

- Entladen Sie PGPdisk-Volumes stets, wenn Sie Ihren Computer verlassen. Auf diese Weise wird der Inhalt sicher in der verschlüsselten, zum Volume gehörigen Datei gespeichert, bis Sie erneut darauf zugreifen.
- Verwenden Sie einen Bildschirmschoner mit einer Paßwort-Option, damit es für andere schwieriger ist, sich Zugang zu Ihrem Rechner zu verschaffen oder Einsicht auf Ihren Bildschirm zu nehmen, wenn Sie nicht an Ihrem Arbeitsplatz sind.
- Stellen Sie sicher, daß Ihre PGPdisk-Volumes nicht von anderen Computern im Netzwerk gesehen werden können. Eventuell müssen Sie dies mit den Mitarbeitern der Netzwerkverwaltung abklären. Auf die Dateien in einem verbundenen PGPdisk-Volume kann jeder zugreifen werden, der sie im Netzwerk sieht.
- Notieren Sie sich nie Ihre Paßphrasen. Wählen Sie etwas, an das Sie sich erinnern können. Wenn Sie Schwierigkeiten haben, sich an Ihre Paßphrase zu erinnern, helfen Sie Ihrem Gedächtnis mit einem Poster, einem Lied, einem Gedicht oder einem Witz auf die Sprünge. *Notieren Sie jedoch nie Ihre Paßphrasen*.
- Wenn Sie PGPdisk zu Hause verwenden und auch andere Personen auf Ihren Computer Zugriff haben, können diese wahrscheinlich Ihre PGPdisk-Dateien anzeigen. Solange Sie die PGPdisk-Volumes entladen, wenn Sie sie nicht mehr verwenden, kann niemand anders deren Inhalt lesen.
- Wenn ein anderer Benutzer über physischen Zugriff auf Ihren Rechner verfügt, kann er sowohl Ihre PGPdisk-Dateien als auch alle anderen Dateien und Volumes löschen. In diesem Fall sollten Sie entweder Sicherheitskopien von Ihren PGPdisk-Dateien erstellen oder sie auf externen Medien speichern, zu denen sich kein anderer physischen Zugang verschaffen kann.

- Denken Sie daran, daß Kopien Ihres PGPdisk-Volumes denselben zugrundeliegenden Verschlüsselungsschlüssel wie das Original verwenden. Wenn Sie eine Kopie Ihres Volumes mit einem anderen Benutzer austauschen und Sie beide Ihre Master-Paßwörter ändern, verwenden Sie und die andere Person immer noch denselben Schlüssel für die Verschlüsselung der Daten. Obwohl es nicht einfach ist, den Schlüssel wiederherzustellen, ist dies nicht unmöglich. Sie können den zugrundeliegenden Schlüssel ändern, indem Sie das PGPdisk-Volume neu verschlüsseln. Weitere Informationen zum Neuverschlüsseln finden Sie im Abschnitt “Eigenschaften für ein PGPdisk-Volume festlegen” auf Seite 160.

Teil IV: Netzwerkkommunikation mit PGPnet sichern

- **Kapitel 9: PGPnet-Grundlagen**
- **Kapitel 10: Kurze Einführung in PGPnet**
- **Kapitel 11: Die PGPnet-Firewall- und -Angrifferkennungsfunktion konfigurieren**
- **Kapitel 12: Die PGPnet-Funktion “VPN” konfigurieren**

PGPnet-Grundlagen 9

Zu PGPnet

Dank der modernen Kommunikationstechnik hat sich der Arbeitsalltag in vielen Bereichen entscheidend verändert. Wurden beispielsweise interne Mitteilungen und Berichte noch vor einigen Jahren in Postfächern abgelegt und erreichten erst nach einigen Tagen die Adressaten, so werden diese heute elektronisch verschickt und gelangen in Bruchteilen von Sekunden an ihren Bestimmungsort. Vor allem Mitarbeiter, die zu Hause arbeiten oder im Außendienst tätig sind, profitieren von der neuen Technik: Sie können per Telefonverbindung problemlos Daten zwischen ihrem Computer und der Firma austauschen.

Doch diese Entwicklung hat zwei Schattenseiten: Zum einen birgt die Übertragung von Daten über Telefonleitungen erhebliche Sicherheitsrisiken in sich, und zum anderen führte sie zu einem signifikanten Anstieg der Telefonkosten. Für viele Unternehmen hat zwar das Internet das Problem der Kosten gelöst, die Sicherheit ist jedoch nach wie vor nicht gewährleistet.

Glücklicherweise bieten jedoch neuere Technologien eine Lösung für dieses Problem. *Persönliche Firewalls* filtern den Datenverkehr, d. h., der Durchgang wird nur solchen Daten gewährt, die den in der Firewall-Software festgelegten Kriterien entsprechen. Außerdem können *Angrifferkennungssysteme* eingesetzt werden, die Angriffe auf einzelne Computer erkennen und abwehren, die Benutzer über die Angriffe informieren und in Zukunft jeglichen Verkehr von den angreifenden Quellen ablehnen. Durch **virtuelle private Netzwerke (VPNs)** können Unternehmen Daten auf sichere Weise über das Internet übertragen. Dadurch wird nicht nur die Gefährdung der Daten bei der Übertragung vermindert, sondern die Telefonkosten können auch drastisch verringert werden.

Diese drei Technologien – persönliche Firewalls, Angrifferkennungssysteme und VPNs – sind in PGPnet, der PGP-Lösung für eine sichere Netzwerkkommunikation, vereint. In diesem Kapitel finden Sie Hintergrundinformationen zu diesen drei PGPnet-Komponenten.

Einen Überblick über die PGPnet-Benutzeroberfläche erhalten Sie in Kapitel 10, “Kurze Einführung in PGPnet”. Informationen dazu, wie Sie die Funktionen von PGPnet konfigurieren können, finden Sie in Kapitel 11, “Die PGPnet-Firewall- und -Angrifferkennungsfunktion konfigurieren”, und Kapitel 12, “Die PGPnet-Funktion “VPN” konfigurieren”.

Was ist eine persönliche Firewall?

Eine persönliche Firewall hat die Funktion eines Filters, der den gesamten Datenverkehr prüft, der an Ihrem Computer ankommt und diesen Computer verläßt. Viele Unternehmen verfügen mittlerweile über einen oder mehrere Firewall-Server, die den gesamten eingehenden und ausgehenden Netzwerkverkehr filtern. Die einzelnen Hosts im Netzwerk können aber weiterhin Angriffen ausgesetzt sein, die aus dem als vertrauenswürdig eingestuften Netzwerk stammen. Da die persönliche Firewall-Software von PGP auf jedem einzelnen Host des Netzwerks installiert wird, schützt sie jeden Host vor Angriffen, die sowohl von innerhalb als auch von außerhalb des Firmen-Netzwerks stammen. Darüber hinaus können die Funktionen der persönlichen Firewall von PGPnet präzise auf den konkreten Bedarf jedes einzelnen Hosts abgestimmt werden.

Die Überprüfung der an Ihrem Computer eingehenden und ausgehenden Daten durch die persönliche Firewall von PGPnet beruht auf bestimmten Firewall-*Regeln*. Diese Regeln wiederum basieren auf fünf Informationssegmenten, die an die Daten angehängt sind:

1. Quelladresse (die IP-Adresse des Computers, von dem die Daten kommen)
2. Zieladresse (die IP-Adresse des Computers, an den die Daten gehen)
3. lokaler Service (der Port bzw. der damit verknüpfte Service auf Ihrem Computer)
4. entfernter Service (der Port bzw. der damit verknüpfte Service auf einem entfernten Computer)
5. Protokoll (z. B. TCP, ICMP und UDP)

Wenn Sie die persönliche Firewall von PGPnet auf Ihrem Computer konfigurieren, können Sie die Firewall-Regeln ganz einfach definieren, indem Sie einen von sechs Schutzgraden wählen : “Keine”, “Minimal”, “Client - Mittel”, “Server - Mittel”, “Client - Hoch” oder “Server - Hoch”. Sie können aber auch einen benutzerdefinierten Schutzgrad wählen.

Durch die Auswahl eines der vordefinierten Schutzgrade für die PGPnet-Firewall lassen Sie die Software die konkreten Einstellungen für die Firewall-Regeln vornehmen. Wenn Sie beispielsweise den Schutzgrad “Minimal” auswählen, gestattet die Software dem Großteil des bei Ihrem Computer ankommenden und ausgehenden Datenverkehrs den Durchgang. Wenn Sie dagegen den Schutzgrad “Client - Hoch” gewählt haben, werden viele Typen des Datenverkehrs gesperrt. (Weitere Informationen zu Unterschieden zwischen den vordefinierten Firewall-Schutzgraden in PGPnet finden Sie in Kapitel 11, “Die PGPnet-Firewall- und -Angrifferkennungsfunktion konfigurieren”.)

Falls Sie sich für das Erstellen eines benutzerdefinierten Schutzgrades entschieden haben, legen Sie mit Hilfe der Software die Einzelheiten für die Firewall-Regeln fest. So könnten Sie beispielsweise zunächst den Schutzgrad “Client - Hoch” wählen und anschließend explizit einen Verkehrstyp zulassen, der ansonsten gesperrt wäre, beispielsweise die Kommunikation mit bestimmten entfernten Hosts.

Genauere Informationen, wie Sie einen persönlichen Firewall in PGPnet konfigurieren können, finden Sie in Kapitel 11, “Die PGPnet-Firewall- und -Angrifferkennungsfunktion konfigurieren”.

Was ist ein Angrifferkennungssystem?

Selbst die besten Firewalls können durch einen hartnäckigen Angreifer umgangen werden. Woher wissen Sie aber, ob Ihr System durch einen Angriff gefährdet wurde? Das Angrifferkennungssystem (Intrusion Detection System, IDS) von PGPnet warnt Sie in einem solchen Fall.

Ein Angrifferkennungssystem tut einfach das, was sein Name sagt: Es erkennt Angriffe. Das Angrifferkennungssystem von PGPnet sucht nach verdächtigen Aktivitäten, beispielsweise nach bestimmten Verkehrsmustern, die typisch sind für Angriffe. Sobald ein Angriffs *ereignis* erkannt wird, erfaßt das IDS dieses Ereignis im Protokoll und zeichnet die Quelladresse des Angreifers auf. Zusätzlich protokolliert IDS den Grund, warum das Ereignis als Angriff bewertet wurde, sowie den Zeitpunkt des Ereignisses. Sie können das IDS auch so konfigurieren, daß beim Erkennen eines Angriffs ein Signalton ertönt, daß per E-Mail eine Warnmeldung and einen Administrator gesendet wird und daß der Angriff sowie der gesamte zukünftige Verkehr des Angreifers blockiert wird.

Das IDS kann auch so konfiguriert werden, daß es mit den Einstellungen Ihrer persönlichen Firewall arbeitet. Sie können eine benutzerdefinierte Firewall-Regel erstellen, die einen bestimmten Verkehrstyp blockiert. Wenn dann an Ihrem Computer Verkehr entsprechend dieser Regel eingeht, betrachtet das IDS dieses Ereignis als Angriff und behandelt es entsprechend.

Genauere Informationen, wie Sie Ihr persönliches Angrifferkennungssystem in PGPnet konfigurieren können, finden Sie in Kapitel 11, “Die PGPnet-Firewall- und -Angrifferkennungsfunktion konfigurieren”.

Was ist ein VPN?

Ein VPN (virtuelles privates Netzwerk) ist eine sichere Kommunikationsverbindung über ein unsicheres Medium, im allgemeinen das Internet. Die Sicherheit der Verbindung wird durch Software gewährleistet, die auf den Computern auf beiden Seiten der Kommunikationsverbindung installiert ist. Diese Software überprüft die Authentizität der Benutzer und führt die Datenverschlüsselung durch. Mit einem VPN können nur legitime Benutzer an der sicheren Datenübertragung teilnehmen, und es ist nicht möglich, die Daten während der Übertragung zu lesen oder gar zu manipulieren.

Ein VPN ist immer dann empfehlenswert, wenn Daten über das Internet gesendet und empfangen werden sollen, bei denen es darauf ankommt, daß sie nicht von anderen gelesen, verändert oder zu betrügerischen Zwecken verwendet werden. Beispiele:

- Remote-Hosts können VPNs zur sicheren Kommunikation mit einem Firmen-Netzwerk verwenden.
- Zwei Firmen-Netzwerke (die beispielsweise zum selben Großunternehmen gehören), die sich in unterschiedlichen geographischen Regionen befinden, können über das VPN als ein gemeinsames Netzwerk betrieben werden.
- Firmen, die VPNs installieren, können diese auch dazu verwenden, ihre internen Daten vertrauenswürdigen Firmen und Einzelpersonen (z. B. Lieferanten, Beratern oder ganz bestimmten Personen innerhalb der Firma) verfügbar zu machen.
- Einzelpersonen, die über das Internet ungestört miteinander kommunizieren möchten, können dazu eine VPN-Verbindung nutzen.

Diese Beispiele zeigen, wie ein VPN mit geringem Kostenaufwand die sichere Übertragung von Daten gewährleisten kann.

Wie funktioniert die VPN-Funktion von PGPnet? Hier ein Beispiel zur Veranschaulichung:

Sie sind ein Benutzer im Firmennetzwerk von Unternehmen A. Von Ihrer Vorgesetzten erfahren Sie, daß Sie mit einem auswärtigen Vertriebskollegen kommunizieren müssen. Bei dieser Kommunikation sollen auch Daten ausgetauscht werden, die als vertraulich gelten. Es gibt aber keinen Grund zur Sorge: Die Kommunikation mit dem Vertriebsmitarbeiter kann über ein VPN erfolgen.

Die Einrichtung einer solchen VPN-Kommunikation ist mit PGPnet problemlos möglich:

1. Sorgen Sie dafür, daß der entfernte Computer (in diesem Beispiel der Computer des Vertriebsmitarbeiters) über eine direkte Leitung oder das Internet eine Verbindung zum Unternehmensnetzwerk herstellen kann.
2. Vergewissern Sie sich, daß sowohl auf Ihrem Computer als auch auf dem entfernten Computer PGP Desktop Security (oder ein kompatibles Produkt) installiert ist.
3. Nehmen Sie den entfernten Computer (über dessen IP-Adresse) in die Liste als Host auf, mit dem Sie über eine VPN-Verbindung kommunizieren möchten.
4. Wählen Sie ein Verfahren zum Verschlüsseln und Authentisieren Ihrer Daten aus, beispielsweise eine gemeinsame geheime Paßphrase oder einen Verschlüsselungsschlüssel.

   (Weitere Informationen zum Erstellen von Schlüsseln finden Sie in Kapitel 3, “Schlüssel erstellen und austauschen”.)

Sobald diese grundlegenden Kriterien erfüllt sind, kann zwischen Ihren beiden Computern automatisch eine sichere Kommunikation erfolgen. Genauere Informationen, wie Sie die VPN-Funktion in PGPnet konfigurieren können, finden Sie in Kapitel 12, “Die PGPnet-Funktion “VPN” konfigurieren”.

VPN-Begriffe

Zwar geht die Einrichtung der VPN-Kommunikation ziemlich reibungslos vonstatten, im Hintergrund laufen dabei jedoch umfangreiche Verhandlungen zwischen den Computern. In der folgenden Liste finden Sie Begriffe und Formulierungen, die häufig im Zusammenhang mit VPNs verwendet werden. Unter Umständen stoßen Sie auf diese Begriffe, wenn Sie mit PGPnet Ihre Netzwerkkommunikation sichern. Sie müssen diesen Abschnitt aber nicht unbedingt lesen. Die darin enthaltenen Informationen sind in erster Linie für Benutzer bestimmt, die mehr über die VPN-Terminologie erfahren möchten.

- *IPsec* (Internet Protocol Security) ist ein Protokoll, das als Standard für die gesicherte Informationsübertragung über unsichere Netzwerke (z. B. das Internet) entwickelt wurde.
- Ein *sicherer Host* ist ein Rechner, auf dem PGPnet oder eine andere IPsec-kompatible, Peer-To-Peer-fähige Client-Software ausgeführt wird (d. h. Software, die es Hosts ermöglicht, direkt miteinander zu kommunizieren).
- Ein *Gateway* ist ein Rechner, der Ihren Computer bzw. Ihr Netzwerk mit anderen Netzwerken verbindet.

- Ein *sicherer Gateway* ist ein Gateway, der über eine Firewall oder eine andere Sicherheitssoftware verfügt. Ein solcher sicherer Gateway läßt nur Datenpakete durch, die von autorisierten Parteien stammen. Als autorisierte Partei gilt jeder, der über ein Zertifikat bzw. eine Paßphrase verfügt, das bzw. die vom Gateway akzeptiert wird. (Wenn Sie PGPnet verwenden, können Sie wählen, ob Sie zur Authentisierung der Kommunikation mit einem Host Ihren PGP-Schlüssel, ein X.509-Zertifikat oder eine gemeinsame Paßphrase verwenden wollen.)
- *Tunnelmodus* ist ein VPN-Modus für die Kommunikation mit Hosts oder Teilnetzen, die sich hinter einem sicheren Gateway befinden.
- *Transportmodus* ist ein VPN-Modus für die Kommunikation zwischen zwei sicheren Hosts, zwischen denen kein Gateway liegt (diese Kommunikation wird auch als *Peer-To-Peer*-Kommunikation bezeichnet).
- Ein *sicheres Teilnetz* ist ein Teilnetz (ein Netzwerk, das wiederum Bestandteil eines größeren Netzwerks ist), das aus bis zu 254 Rechnern besteht, auf denen normalerweise PGPnet oder eine kompatible Client-Software ausgeführt wird. Die Zuordnung eines sicheren Teilnetzes ermöglicht es Ihnen (bzw. Ihrem Administrator), mehrere Rechner im gleichen IP-Adreßbereich zu ermitteln, die IPsec-kompatibel sind. Beachten Sie bitte, daß sich sichere Teilnetze nicht hinter Gateways befinden müssen.
- Ein *unsicherer Host* ist ein Rechner, auf dem weder PGPnet noch eine andere IPsec-kompatible und Peer-To-Peer-fähige Client-Software ausgeführt wird.
- Ein *unsicheres Teilnetz* ist ein Teilnetz, das aus bis zu 254 Rechnern besteht, auf denen weder PGPnet noch eine kompatible Client-Software ausgeführt wird.
- Eine *Sicherheitsverknüpfung (Security Association, SA)* ist eine Übereinkunft über die Bedingungen einer sicheren Kommunikation zwischen zwei Rechnern. Eine SA wird erstellt, wenn ein lokaler Rechner erstmalig mit einem entfernten Rechner (Remote-Rechner) kommuniziert. Sie beschreibt, wie die beiden Rechner miteinander kommunizieren (z. B. den verwendeten Verschlüsselungstyp, die Gültigkeitsdauer der Verknüpfung, die Authentisierungsmethode).

  Alle SAs, die Ihr Rechner aufbaut und die von anderen Rechnern mit Ihrem Rechner aufgebaut werden, werden von PGPnet aufgezeichnet und überwacht. Wenn sich eine von Ihrem Rechner aufgebaute SA dem Ablaufdatum nähert, baut PGPnet mit dem entfernten Host eine neue SA auf.

HINWEIS: Sie können sämtliche aktiven SAs auf der PGPnet-Registerkarte **Status** anzeigen lassen. Weitere Informationen zur Registerkarte **Status** finden Sie unter siehe “Status der vorhandenen Sicherheitsverbindungen (SAs) überprüfen” auf Seite 189.

- *IKE (Internet Key Exchange)* ist eine sichere Möglichkeit, Schlüssel über das Internet auszutauschen.

Kurze Einführung in PGPnet 10

In diesem Kapitel erhalten Sie einen kurzen Überblick über PGPnet und die PGPnet-Benutzeroberfläche.

PGPnet starten

Für das Starten von PGPnet gibt es folgende zwei Möglichkeiten:

- Wählen Sie **Start—>Programme—>PGP—>PGPnet**.

  oder

- Starten Sie PGPnet von PGPtray in der Systemleiste der Windows-Taskleiste (**PGPtray—>PGPnet—>Status, VPN, Einbrecher oder Protokoll**).

Bei beiden Methoden wird die Registerkarte **PGPnet** geöffnet.

PGPnet aktivieren und deaktivieren

Wenn PGPnet aktiviert ist, wird die Anwendung im Hintergrund ausgeführt. Verwenden Sie Ihre Software (z. B. E-Mail oder Browser) wie gewohnt, um mit einem anderen Rechner zu kommunizieren. PGPnet bewertet jeden Kommunikationsvorgang und nimmt Verschlüsselung und Tunneling wie erforderlich vor.

Verwenden Sie die Schaltfläche in der oberen rechten Ecke des Hauptfensters von PGPnet, um PGPnet zu aktivieren und zu deaktivieren (siehe Abbildung 10-1 auf Seite 184).

- Wenn PGPnet jedoch deaktiviert ist und der Rechner neu gestartet wird, ist PGPnet nach dem Neustart deaktiviert.
- Wenn PGPnet deaktiviert ist, kann der Datenverkehr mit allen Computern ohne Verschlüsselung oder sonstige Veränderungen passieren.

Abbildung 10-1. PGPnet aktivieren und deaktivieren

PGPnet beenden

Wählen Sie im PGPnet-Menü **Datei** den Befehl **Beenden** , oder klicken Sie in der rechten oberen Ecke des PGPnet-Fensters auf die Schaltfläche mit dem **X**.

PGPnet-Funktionen

Thema:	Siehe:
Informationen zum PGPtray-Symbol	“Das PGPtray-Symbol” auf Seite 185
Überblick über das PGPnet-Fenster	“Das PGPnet-Fenster auf einen Blick” auf Seite 186
Status der vorhandenen Sicherheitsverbindungen (SAs) überprüfen	“Status der vorhandenen Sicherheits-verbindungen (SAs) überprüfen” auf Seite 189
SAs einrichten und beenden	“SAs einrichten und beenden” auf Seite 192
Kommunikation mit anderen Rechnern blockieren	“Kommunikation mit anderen Rechnern blockieren” auf Seite 193
Überblick über die Einträge auf der PGPnet-Registerkarte “Protokoll”	“PGPnet-Protokolleinträge anzeigen” auf Seite 197
sichere Netzwerkschnittstelle ändern	“Sichere Netzwerkschnittstelle ändern: “PGPnet – Adapter einstellen”” auf Seite 198

Das PGPtray-Symbol

Das PGPtray-Symbol gibt Ihnen den Status von PGPnet an.

Symbol	Beschreibung	PGPnet-Status
	Graues Schloß.	PGPnet ist entweder deaktiviert oder wurde nicht installiert.
	Graues Schloß im Netzwerk.	PGPnet wurde installiert und ist aktiviert.
	Graues Schloß im Netzwerk mit einem Ausrufezeichen im gelben Kreis.	PGPnet wurde installiert, wird jedoch nicht ausgeführt.
	Gelbes Schloß im Netzwerk mit einem grünen Netzwerkanschluß.	PGPnet ist installiert und aktiviert und verfügt über aktive SAs. Der QuickInfo-Text gibt die Anzahl der SAs an. Während PGPnet eine SA aushandelt, blinkt der grüne Netzwerkstecker.
	Graues Schloß im Netzwerk mit blinkendem roten Ausrufezeichen. Das Ausrufezeichen blinkt so lange, bis Sie den Mauszeiger über das PGPtray-Symbol bewegen. Wenn Sie bei blinkendem Ausrufezeichen auf das PGPtray-Symbol klicken, wird entweder die Registerkarte **Einbrecher** (wenn die automatische Blockierungsfunktion von IDS aktiv ist) oder die Registerkarte **Protokoll** angezeigt (wenn die automatische Blockierungsfunktion von IDS nicht aktiv ist).	PGPnet ist installiert und aktiviert und hat einen Angriff erkannt.

Abbildung 10-2. Das PGPtray-Symbol

Wenn Sie mit dem Mauszeiger auf das PGPtray-Symbol zeigen, erscheint eine QuickInfo mit Informationen zum Status von PGPnet sowie Beschreibungen von Fehlermeldungen (z. B. “Service wird nicht ausgeführt” oder “Treiber nicht installiert”).

Das PGPnet-Menü in PGPtray zeigt die Hosts auf der Registerkarte VPN an. Hosts mit SAs werden mit einem grünen Punkt gekennzeichnet.

- Um eine Verbindung aufzubauen, klicken Sie auf einen Host ohne SA.
- Um eine SA zu beenden, klicken Sie auf einen Host mit einer SA.

Das PGPnet-Fenster auf einen Blick

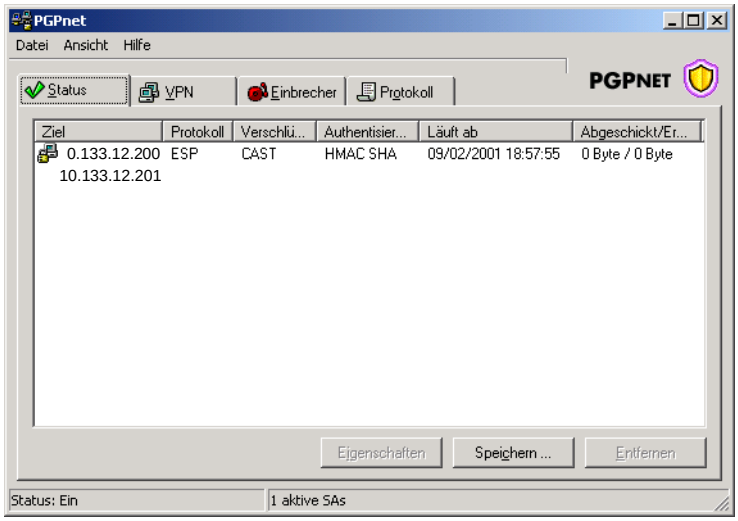


Abbildung 10-3. Das PGPnet-Fenster

Menüs

Im PGPnet-Fenster gibt es die folgenden drei Menüs:

- **Datei** (**Speichern**, **Hosts exportieren**, **Hosts importieren**, **PGPnet aktivieren**, **PGPnet deaktivieren** und **Beenden**)
- **Ansicht** (**Status**, **VPN**, **Einbrecher**, **Protokoll** und **Optionen**)
- **Hilfe** (**Inhalt und Index** und **Info**)

Registerkarten

Das PGPnet-Fenster enthält die folgenden vier Registerkarten:

- **Registerkarte Status:** Verwenden Sie diese Registerkarte, um den Status der vorhandenen Sicherheitsverbindungen (SAs) zu überprüfen (siehe “Status der vorhandenen Sicherheitsverbindungen (SAs) überprüfen” auf Seite 189).

- **Registerkarte VPN:** Verwenden Sie diese Registerkarte, um der PGPnet-Hostliste Einträge hinzuzufügen, die vorhandenen Einträge zu bearbeiten oder zu entfernen. Diese Registerkarte dient auch zum manuellen Herstellen und Beenden von SAs. Denken Sie daran, daß Sie, nachdem Sie Hosts der Hostliste hinzugefügt haben, SAs auch vom PGP-Menü in PGPtray aus herstellen und beenden können.

  Neben dem manuellen Hinzufügen von Einträgen zur Liste können Sie eine PGPnet-Hostliste auch per Drag & Drop vom Desktop auf die **Registerkarte VPN** ziehen.

  Wenn links von einem Eintrag in der Hostliste ein Pluszeichen (+) angezeigt wird, klicken Sie auf das Pluszeichen, um die Anzeige zu erweitern und andere mit diesem Eintrag verknüpfte Einträge anzuzeigen. Wenn Sie einen Eintrag bearbeiten möchten, doppelklicken Sie auf den Hosteintrag, oder wählen Sie den Eintrag aus, und klicken Sie auf **Eigenschaften**. Mit den Schaltflächen **Verbinden** und **Trennen** können Sie SAs einrichten bzw. beenden. (siehe “SAs einrichten und beenden” auf Seite 192).

- **Registerkarte Einbrecher:** Auf dieser Registerkarte werden die von der Firewall-Funktion von PGPnet blockierten Kommunikationswege angezeigt. Hier können Sie auch Hosts manuell in die Liste der blockierten Hosts einfügen oder Hosts aus dieser Liste entfernen (siehe “Kommunikation mit anderen Rechnern blockieren” auf Seite 193).

- **Registerkarte Protokoll:** Auf dieser Registerkarte finden Sie protokollierte Ereignismeldungen, mit deren Hilfe Sie etwaige Probleme diagnostizieren können (siehe “PGPnet-Protokolleinträge anzeigen” auf Seite 197).

Statusleiste

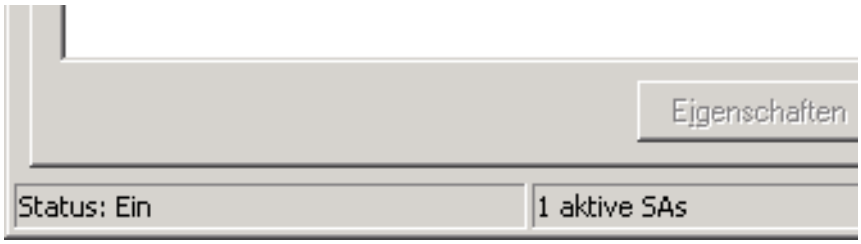


Abbildung 10-4. PGPnet-Statusleiste

In der Statusleiste am unteren Rand des PGPnet-Fensters werden Meldungen angezeigt, die sich auf den Status von PGPnet (links) und auf die Anzahl der aktiven SAs (rechts) beziehen.

In der Statusleiste können die folgenden Meldungen angezeigt werden:

Meldung:	Beschreibung:
Status: Ein	PGPnet ist eingeschaltet.
Status: Aus	PGPnet ist ausgeschaltet.
Treiber nicht installiert	Der PGPnet-Treiber reagiert nicht auf den Service. Starten Sie Ihr System neu. Wenn der Treiber auch dann nicht reagiert, installieren Sie PGPnet erneut. Wenn PGPnet diese Meldung weiterhin anzeigt, setzen Sie sich mit dem Technischen Support von NAI in Verbindung.
Service wird nicht ausgeführt	Der PGPnet-Service wird nicht ausgeführt. Starten Sie Ihr System neu. Wenn PGPnet diese Meldung weiterhin anzeigt, installieren Sie PGPnet erneut. Wenn das Problem durch diese Maßnahmen nicht gelöst wird, setzen Sie sich mit dem Technischen Support von NAI in Verbindung.
Service antwortet nicht	Der PGPnet-Service wird ausgeführt, reagiert jedoch nicht auf Nachrichten von der Anwendung. Starten Sie Ihr System neu. Wenn PGPnet diese Meldung weiterhin anzeigt, installieren Sie PGPnet erneut. Wenn das Problem durch diese Maßnahmen nicht gelöst wird, setzen Sie sich mit dem Technischen Support von NAI in Verbindung.

Status der vorhandenen Sicherheitsverbindungen (SAs) überprüfen

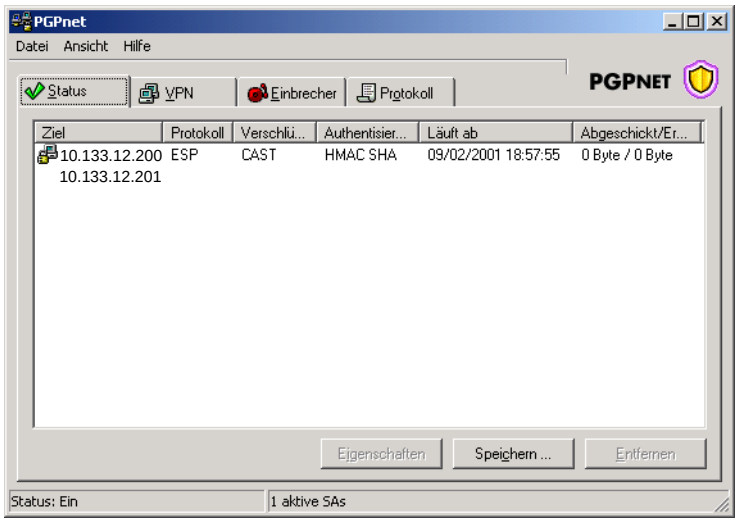


Abbildung 10-5. Registerkarte “Status”

Auf der Registerkarte **Status** im PGPnet-Fenster werden die aktiven SAs aufgelistet (siehe Abbildung 10-5 auf Seite 189). Eine SA wird unter Umständen beendet, wenn ihr Umfang einen bestimmten Wert in Byte erreicht (es werden z. B. 4 MB Daten über die SA übertragen) bzw. wenn ein bestimmter Zeitraum vergangen ist. Die Länge einer SA wird bei ihrem Aufbau abgestimmt. Bei der Abstimmung der SA wird ein Ablaufwert für die Gültigkeit festgelegt. Wenn die SA diesen Ablaufwert erreicht und ungültig wird, wird automatisch eine neue SA erstellt. Der Ablaufwert der Gültigkeit für die SA kann vom Benutzer konfiguriert werden. Weitere Informationen dazu finden Sie unter “VPN-Schlüsselaktualisierung” auf Seite 265.

- Wenn Ihr Rechner eine SA initialisiert, deren Gültigkeit abläuft, wird von PGPnet automatisch die Abstimmung einer neuen SA initialisiert, um die ungültige zu ersetzen. Folglich kann es vorkommen, daß auf der Registerkarte **Status** zeitweise zwei SAs für denselben Rechner angezeigt werden.

- Wenn Sie eine SA mit einem anderen Host erstellen, verwendet PGPnet den jeweils niedrigeren Ablaufwert der beiden Hosts. Folglich wird eine SA möglicherweise ungültig, bevor der maximale Ablaufwert erreicht wird, weil für den anderen Host restriktivere Ablaufwerte festgelegt sind.

Mit Hilfe der Funktion **Speichern** können Sie Listen aktiver SAs in einer Textdatei (mit Tabulatoren als Trennzeichen) speichern.

Mit der Funktion **Entfernen** können Sie eine SA entfernen. Das Entfernen einer SA empfiehlt sich, wenn Sie sie nicht mehr für sicher halten, wenn Sie wissen, daß der Ziel-Host ausgefallen ist, oder wenn Sie aus einem anderen Grund der Ansicht sind, daß die Verbindung nicht mehr aufrechterhalten werden sollte. Diese Schaltfläche ist deaktiviert, wenn PGPnet ausgeschaltet ist.

Mit Hilfe der Funktion **Eigenschaften** können Sie Detailinformationen zu einer SA anzeigen, darunter IP-Adresse, gesendete Bytes, Verschlüsselungstyp usw. Wenn Sie Details sehen möchten, markieren Sie den Host, und klicken Sie anschließend auf **Eigenschaften** (siehe Abbildung 10-6**)**. Klicken Sie auf die Pin-Nadel in der rechten oberen Ecke, wenn das Fenster weiterhin auf Ihrem Bildschirm angezeigt werden soll. Wenn das Fenster offen ist und Sie es schließen möchten, klicken Sie auf das X in der rechten oberen Ecke oder auf **Schließen**.

Mit der Funktion **Automatisch konfigurieren** können Sie einen Host auf der Grundlage einer vorhandenen SA konfigurieren.

- Wenn die SA für einen konfigurierten Host steht, importiert PGPnet den Authentisierungsschlüssel der SA in Ihren PGP-Schlüsselbund und weist diesen Schlüssel als Authentisierungsschlüssel für den konfigurierten Host zu.
- Wenn die SA für einen unkonfigurierten Host steht, erstellt PGPnet in der Hostliste einen neuen Eintrag für einen sicheren Host, importiert den Authentisierungsschlüssel der SA in Ihren PGP-Schlüsselbund und weist diesen Schlüssel als Authentisierungsschlüssel für den konfigurierten Host zu.

Wenn der SA kein Authentisierungsschlüssel zugeordnet ist (d. h., sie verwendet zur Authentisierung eine gemeinsame geheime Paßphrase), können Sie diese Funktion nicht nutzen.

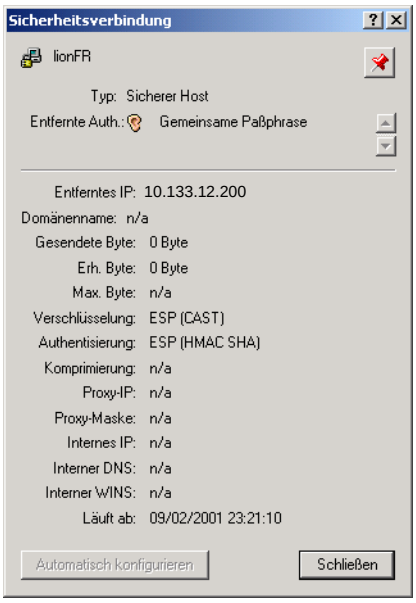


Abbildung 10-6. Eigenschaften einer Sicherheitsverbindung

SAs einrichten und beenden

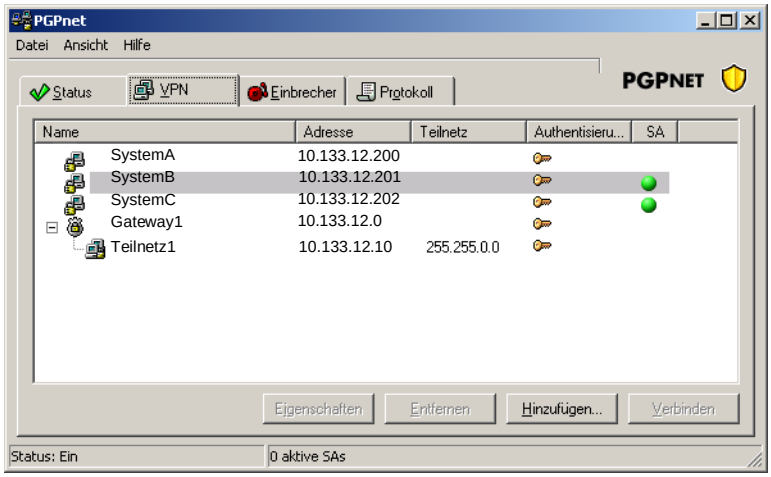


Abbildung 10-7. Registerkarte “VPN”

Auf der **Registerkarte VPN** werden sichere Gateways, Teilnetze und Hosts aufgeführt. Wenn links neben einem Element ein Pluszeichen (+) angezeigt wird, klicken Sie darauf, um die Anzeige zu erweitern und weitere mit dem Element verbundene Einträge einzusehen (siehe Abbildung 10-7 auf Seite 192).

Wenn PGPnet deaktiviert ist, werden alle Schaltflächen abgeblendet dargestellt.

Richten Sie über die Schaltfläche **Verbinden** eine SA mit einem konfigurierten Host ein. Wählen Sie den Host aus, und klicken Sie anschließend auf **Verbinden**. Die Schaltfläche **Verbinden** steht nicht zur Verfügung, wenn ein unzulässiger Host-Eintrag ausgewählt wurde (z. B. wenn Sie ein sicheres Teilnetz oder einen unsicheren Host wählen, der sich nicht hinter einem Gateway befindet).

Wenn Sie eine Verbindung zu einem exklusiven Gateway herstellen, bleiben alle vorhandenen SAs für Hosts, die sich nicht im lokalen Teilnetz befinden, zwar weiter bestehen, werden aber ungültig. Sie können zu jedem Zeitpunkt immer nur eine Verbindung zu einem exklusiven Gateway herstellen.

Klicken Sie auf **Eigenschaften**, um einen Eintrag zu bearbeiten.

Verwenden Sie die Schaltfläche **Trennen**, um eine SA mit einem konfigurierten Host zu beenden. Wählen Sie den Host aus, und klicken Sie anschließend auf **Trennen**.

Hostliste importieren

Zum Importieren einer vorhandenen PGPnet-Hostliste und zum Hinzufügen der Hosts zur Registerkarte **VPN** stehen Ihnen zwei Möglichkeiten zur Verfügung:

- Ziehen Sie die Hostliste direkt vom Desktop auf die PGPnet-Registerkarte **VPN**.
- Wählen Sie den Befehl **Hosts importieren** aus dem PGPnet-Menü **Datei**, gehen Sie zu der zu öffnenden Datei, wählen Sie sie aus, und klicken Sie auf **Öffnen**.

Hostliste exportieren

So exportieren Sie eine Hostliste:

1. Wählen Sie im PGPnet-Menü **Datei** den Befehl **Host exportieren**.
2. Speichern Sie die Hostliste als .txt-Datei, beispielsweise **hostList0400.txt**.

Kommunikation mit anderen Rechnern blockieren

Auf der PGPnet-Registerkarte **Einbrecher** werden alle Hosts angezeigt, für die die Kommunikation mit Ihrem System blockiert ist. Außerdem wird angezeigt, warum diese Hosts blockiert sind und wie lange sie noch blockiert sein werden.

Mit Hilfe der Optionen auf dieser Registerkarte können Sie andere Systeme daran hindern, mit Ihrem System zu kommunizieren. Außerdem können Sie von hier aus die Funktion **Quelle aufzeichnen** aufrufen (dabei wird der Weg der Kommunikation von Ihnen zurück zur Quelle verfolgt) und Hosts aus der Liste der blockierten Hosts entfernen.

Wenn ein Host Ihr System angreift und Sie die von diesem Host ausgehende Kommunikation blockieren, können Sie mit Hilfe der Funktion **Quelle aufzeichnen** versuchen, sich Informationen zum Angreifer zu beschaffen. Weitere Informationen dazu finden Sie im Abschnitt “Angreifer aufspüren” auf Seite 195.

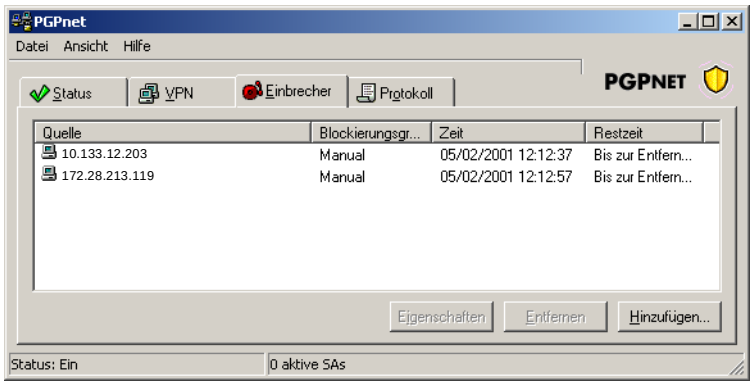


Abbildung 10-8. Registerkarte “Einbrecher”

Über die Schaltfläche **Eigenschaften** können Sie sich Details zum blockierten Host anzeigen lassen. Dazu müssen Sie den blockierten Host markieren und anschließend auf **Eigenschaften** klicken.

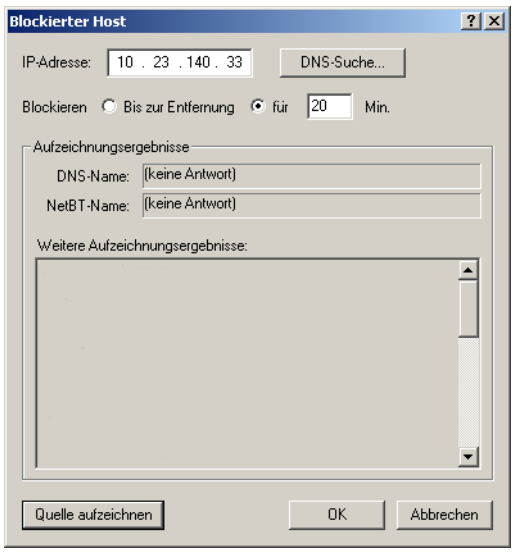


Abbildung 10-9. Dialogfeld “Blockierter Host”

Mit Hilfe von **Entfernen** können Sie einen Host aus der Liste der blockierten Hosts entfernen (siehe “Hosts aus der Liste der blockierten Hosts entfernen” auf Seite 197).

Mit Hilfe von **Hinzufügen** können Sie einen Host in die Liste der blockierten Hosts aufnehmen (siehe “Hosts blockieren und die Kommunikationsquelle zurückverfolgen” auf Seite 195).

Mit Hilfe von **DNS-Suche** können Sie die IP-Adresse eines Hosts feststellen.

Hosts blockieren und die Kommunikationsquelle zurückverfolgen

So blockieren Sie die von einer bestimmten IP-Adresse ausgehende Kommunikation:

1. Klicken Sie auf **Hinzufügen**. PGPnet zeigt daraufhin das Dialogfeld “Blockierter Host” an.
2. Geben Sie die IP-Adresse des Computers ein, den Sie blockieren möchten, oder klicken Sie auf **DNS-Suche**, um die IP-Adresse herauszufinden.
3. Klicken Sie auf **Bis zur Entfernung** oder auf **für [ ] Min.**, und geben Sie die Anzahl der Minuten ein.
4. Klicken Sie auf **OK**.

Angreifer aufspüren

Wenn ein Host Ihr System angreift und er zum blockierten Host wird, können Sie mit Hilfe der PGPnet-Funktion **Quelle aufzeichnen** (siehe Abbildung 10-10 auf Seite 196) versuchen, sich die folgenden Informationen zum Angreifer zu beschaffen: DNS-Name, NetBIOS-Information, TELNET-Banner, HTTP-Serverversion, WHOIS, traceroute, FTP-Serverbanner und SMTP-Banner. (Ein *Banner* ist eine Textzeichenfolge, die die Serversoftware an den Client sendet, wenn der Client erstmals Kontakt mit dem Server aufnimmt. Banner enthalten oft Informationen, aus denen der Server oder das Betriebssystem hervorgeht, das auf dem Server läuft.)

- Wenn die Funktion **Quelle aufzeichnen** den NetBIOS-Namen identifiziert, versucht sie auch, die Netzwerk-Adressen (MAC) dieses Computers zu identifizieren.
- Wenn es der Funktion **Quelle aufzeichnen** gelingt, den DNS-Namen zu identifizieren, fragt sie die WHOIS-Datenbank nach Informationen zur Domäne ab.
- Wenn sie den DNS-Namen nicht identifizieren kann, versucht sie, die DNS-Namen benachbarter IP-Adressen zu identifizieren.

Mit Hilfe dieser Informationen können Sie den Angreifer identifizieren und lokalisieren und versuchen, den Rechner herunterzufahren oder den Angreifer zu verwarnen.

HINWEIS: Um die traceroute-Funktion von **Quelle aufzeichnen** verwenden zu können, muß auf Ihrem Computer Winsock2 installiert sein. Unter Windows NT oder Windows 2000 müssen Sie über Administratorrechte verfügen, um diese Funktion nutzen zu können.

So spüren Sie die Quelle der von einem Angreifer gesendeten Pakete auf:

1. Wählen Sie auf der Registerkarte **Einbrecher** den Hosteintrag aus, und klicken Sie auf **Eigenschaften**.
2. Klicken Sie auf **Quelle aufzeichnen**. PGPnet zeigt im Feld **Weitere Aufzeichnungsergebnisse** alle eingeholten Informationen an. Nach Abschluß der Aufzeichnung ist die Schaltfläche **Quelle aufzeichnen** wieder aktiviert.

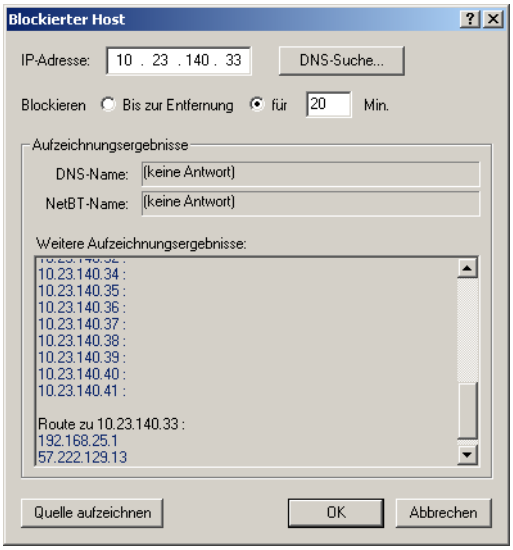


Abbildung 10-10. Dialogfeld “Blockierter Host”: Funktion “Quelle aufzeichnen”

Hosts aus der Liste der blockierten Hosts entfernen

So entfernen Sie einen Host aus der Liste der blockierten Hosts:

1. Wählen Sie den Host aus.
2. Klicken Sie auf **Entfernen**. Sie werden von PGPnet gefragt: “Sollen die ausgewählten Hosts aus der Liste der blockierten Hosts entfernt werden?”
3. Klicken Sie auf **Ja**.

PGPnet-Protokolleinträge anzeigen

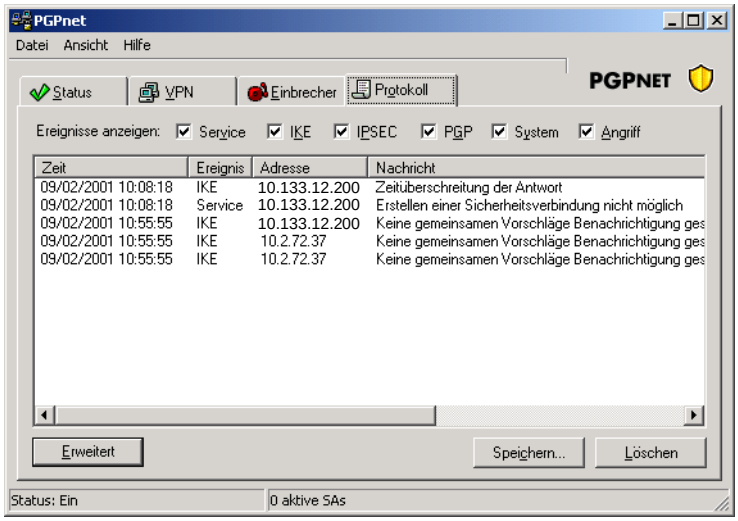


Abbildung 10-11. Registerkarte “Protokoll”

Auf der Registerkarte **Protokoll** werden **Service**-, **IKE**-, **IPSEC**-, **PGP**-, **System**- und **Angreifer**-Ereignisse mit Datum und Uhrzeit sowie einer Beschreibung des Ereignisses oder des Angriffs angezeigt. Diese Informationen unterstützen Sie bei der Behebung auftretender Probleme (siehe Abbildung 10-11 oben). Einträge in Zusammenhang mit Angriffen sind rot markiert.

Aktivieren Sie unter **Ereignisse anzeigen** die Ereignisarten, die angezeigt werden sollen. Wenn Sie PGPnet anweisen möchten, eine bestimmte Art von Ereignis anzuzeigen, markieren Sie das Kontrollkästchen neben dem jeweiligen Ereignistyp. Standardmäßig sind alle Kontrollkästchen markiert.

Klicken Sie auf **Erweitert**, um die IKE-Protokolldatei anzuzeigen. Beachten Sie, daß PGPnet die Daten nicht speichert, wenn Sie das Fenster “Erweitertes IKE-Protokoll” schließen.

Klicken Sie auf **Speichern**, um die Informationen im aktuellen Protokoll in einer Textdatei zu speichern.

Klicken Sie auf **Löschen**, um die Informationen im aktuellen Protokoll aus der Protokolldatei und vom Bildschirm zu löschen. Wenn PGPnet nicht jedesmal beim Löschen des Protokolls um eine Bestätigung bitten soll, klicken Sie auf **Nicht mehr anfragen**.

Sichere Netzwerkschnittstelle ändern: “PGPnet – Adapter einstellen”

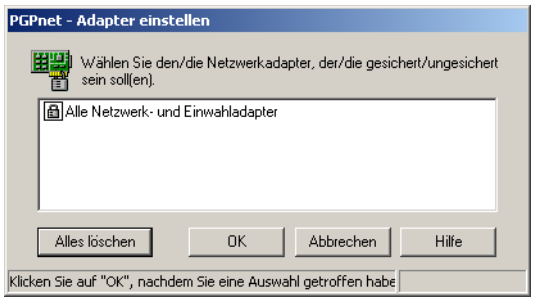


Abbildung 10-12. Dialogfeld “PGPnet – Adapter einstellen”

Bei der Installation von PGPnet werden Sie aufgefordert, die zu sichernden Netzwerkschnittstellen auf Ihrem Computer auszuwählen. Bei der Netzwerkschnittstelle handelt es sich normalerweise um eine Ethernet-Karte, einen DFÜ- oder einen Remote Access WAN-Adapter (steht für Ihr Modem).

Verwenden Sie die PGPnet-Funktion “Adapter einstellen” (**Start—> Programme—>PGP—> SetAdapter**) in den folgenden Situationen:

- Wenn Sie eine andere oder eine zusätzliche Netzwerkschnittstelle sichern möchten.
- Wenn Ihr Rechner das Netzwerkprotokoll und die Adapter-Bindungen überprüft. In diesem Fall wird Ihnen von PGPnet empfohlen, das System neu zu starten und die PGPnet-Funktion “SetAdapter” auszuführen, um eine oder mehrere Netzwerkschnittstellen neu zu sichern.

HINWEIS: Unter Windows 2000 zeigt “SetAdapter” “Alle Netzwerk- und DFÜ-Adapter” an. Durch diese Option werden sämtliche Netzwerkschnittstellen gesichert.

HINWEIS: Wenn Sie auf Windows 98-Computern mehrere Netzwerkschnittstellen sichern, werden im Dialogfeld “Netzwerk” der Systemsteuerung mehrere PGPnet-Adapter angezeigt.

WARNUNG: Wenn Sie nach dem Neustart von PGPnet aufgefordert werden, die Funktion “Adapter einstellen” auszuführen, müssen Sie dieser Aufforderung unbedingt nachkommen. Andernfalls werden keine Netzwerkadapter gesichert und PGPnet funktioniert nicht.

So sichern Sie eine andere oder eine zusätzliche Netzwerkschnittstelle (Windows 95/98):

1. Wählen Sie **Start—>Programme—>PGP—>SetAdapter**. Das Dialogfeld “PGPnet – Adapter einstellen” mit einer Liste aller Adapter wird angezeigt.
2. Wählen Sie die entsprechende Netzwerkschnittstelle, und klicken Sie anschließend auf **OK**. PGPnet fordert Sie auf, Ihren Rechner neu zu starten.
3. Starten Sie Ihr System neu. Dies ist für das Funktionieren des Netzwerks unbedingt erforderlich.

So sichern Sie eine andere oder eine zusätzliche Netzwerkschnittstelle (Windows NT):

1. Wählen Sie **Start—>Programme—>PGP—>SetAdapter**. Das Dialogfeld “PGPnet – Adapter einstellen” mit einer Liste aller Adapter wird angezeigt.
2. Wählen Sie die entsprechende Netzwerkschnittstelle, und klicken Sie anschließend auf **OK**. PGPnet fordert Sie auf, Ihren Rechner neu zu starten.
3. Starten Sie Ihr System neu. Dies ist für das Funktionieren des Netzwerks unbedingt erforderlich.

So sichern Sie eine Netzwerkschnittstelle nach einer Bindungsüberprüfung erneut (Windows NT):

1. Starten Sie den Rechner neu, wenn Sie dazu aufgefordert werden.
2. Beim Neustart wird **SetAdapter** automatisch gestartet, und Sie werden aufgefordert, einen Adapter für die Bindung mit PGPnet auszuwählen.
3. Wählen Sie die entsprechende Netzwerkschnittstelle aus. PGP überprüft die Bindungen Ihres Rechners und fordert Sie auf, Ihren Rechner neu zu starten.
4. Starten Sie Ihr System neu. Dies ist für das Funktionieren des Netzwerks unbedingt erforderlich.

Die PGPnet-Firewall- und -Angrifferkennungsfunktion konfigurieren

11

Firewalls zählen heute zu den gängigen Bestandteilen von Unternehmensnetzwerken. Mit einer *Firewall* wird festgelegt, welche Rechner im Netzwerk des Unternehmens für externe Hosts “sichtbar” sind und auf welche Dienste der Host zugreifen kann. Außerdem kann mit einer Firewall festgelegt werden, welche Computer im Internet für einen Host im unternehmensinternen Intranet “sichtbar” sind und auf welche Dienste der Host Zugriff hat. Firewalls schützen Unternehmensnetzwerke und deren Computer sowie Firmengeheimnisse und vertrauliche Kundendaten vor unberechtigtem Zugriff.

Die Firewall von PGPnet bietet kleinen Büros, die nicht über eine eigene Unternehmens-Firewall verfügen, einen optimalen Firewall-Schutz. Sie gewährleistet auch den Schutz von Firmenbenutzern, wenn diese außerhalb der Unternehmens-Firewall arbeiten, etwa zu Hause oder im Außendienst. Innerhalb der Unternehmens-Firewall sind die Benutzer vor Angriffen geschützt, die aus dem Firmennetzwerk stammen. Dabei profitieren Benutzer, die zu Hause arbeiten, genauso von der Firewall wie die Benutzer im Unternehmen.

Neue Sicherheitsfragen ergeben sich aus der Breitbandkommunikation beispielsweise über DSL oder Kabelmodems. Bei diesen neuartigen Verbindungstypen können Sie 24 Stunden täglich mit dem Internet verbunden sein. Damit ist Ihr Computer jedoch auch ständigen Angriffen ausgesetzt, selbst wenn Sie gar nicht im Internet aktiv sind. Die Firewall und das Angrifferkennungssystem von PGPnet sorgen im Hintergrund dafür, daß Ihr Computer jederzeit geschützt ist. Sie blockieren unnötigen Verkehr und geben entsprechende Warnungen aus, wenn der eingehende Datenverkehr verdächtig ist.

Die PGPnet-Firewall umfaßt eine Reihe von vordefinierten Firewall-Schutzgraden, mit denen Sie festlegen können, welche Pakettypen Ihr Computer empfangen darf und über welche Ports der Empfang dieser Pakete erfolgen soll. Wenn Ihr Computer als Server arbeitet, können Sie festlegen, welche Pakete über welche Ports gesendet werden.

Sie können auch eigene Schutzregeln erstellen und so bestimmte Protokolle, Dienste und Adressen sperren oder zulassen. Wenn Sie eine benutzerdefinierte Regel erstellen, die einen bestimmten Verkehrstyp sperrt (z. B. eingehende ICMP-Pakete), können Sie festlegen, daß PGPnet bei der Erkennung von Verkehr, der den Filterkriterien der Regel entspricht (in diesem Fall ICMP-Pakete), diesen Verkehr als Angriff bewertet und entsprechend behandelt. (Die zugehörige Option “Regelübereinstimmung als Angriff behandeln” finden Sie im Dialogfeld “Firewall-Regel”, wenn Sie eine benutzerdefinierte Regel erstellen.)

Außerdem können Sie festlegen, daß alle Pakete, die von einem bestimmten Host ausgehen, blockiert werden und daß versucht werden soll, die Quelle der von blockierten Hosts ausgehenden Pakete zu ermitteln.

Dabei ist folgendes zu beachten:

- Jeder Verkehr, der nicht durch eine Regel erlaubt wird, wird gesperrt.
- Wenn keiner der vordefinierten Schutzgrade gewählt wird und auch keine benutzerdefinierten Regeln konfiguriert werden, wird der gesamte Netzwerkverkehr gesperrt.
- Die Regeln werden in der Reihenfolge angewendet, in der Sie in der Liste aufgeführt werden (von oben nach unten).
- Eingehende und ausgehende Verbindungen werden auf der Basis der bestehenden Firewall-Regeln zum Zeitpunkt des Verbindungsaufbaus zugelassen oder aber gesperrt. Eine Änderung der Firewall-Regeln, während Verbindungen bestehen, wird erst bei allen anschließend aufgebauten Verbindungen wirksam.

Die persönliche Firewall in PGPnet konfigurieren

Verwenden Sie zum Konfigurieren der persönlichen Firewall in PGPnet die Registerkarte **Persönliche Firewall** des Dialogfelds “PGP-Optionen”. (Klicken Sie dazu auf das PGPtray-Schloßsymbol, wählen Sie **Optionen**, und klicken Sie dann auf die Registerkarte **Persönliche Firewall**.)

Zum Konfigurieren der Firewall können Sie entweder die in PGPnet vordefinierten Schutzgrade verwenden oder aber eigene Schutzgrade erstellen.

- Informationen dazu, wie Sie die persönliche Firewall unter Verwendung eines vordefinierten Schutzgrades konfigurieren können, finden Sie im Abschnitt “Vordefinierten Schutzgrad verwenden” auf Seite 203.
- Informationen dazu, wie Sie die persönliche Firewall durch Erstellen eines benutzerdefinierten Schutzgrades konfigurieren können, finden Sie im Abschnitt “Benutzerdefinierten Schutzgrad erstellen” auf Seite 209.

Vordefinierten Schutzgrad verwenden

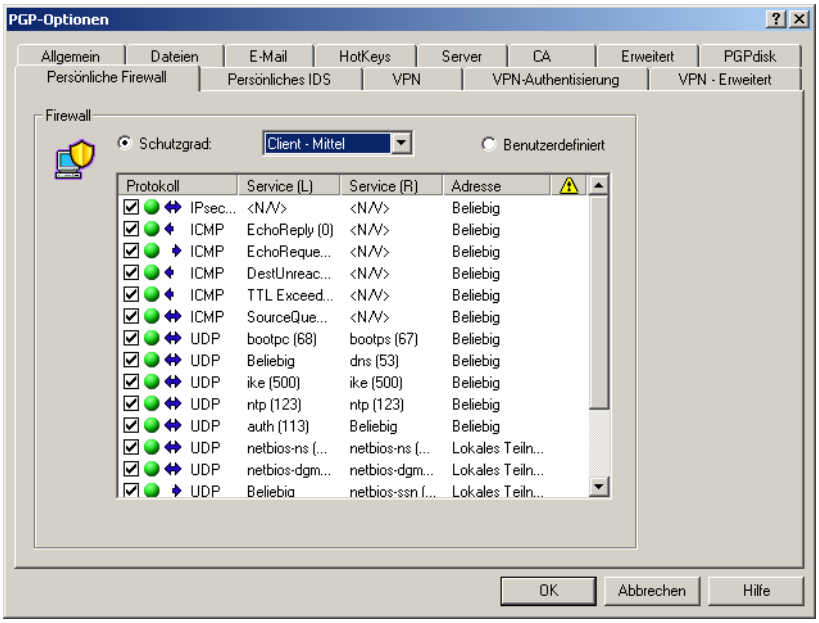


Abbildung 11-1. Dialogfeld “PGP-Optionen” (Registerkarte “Persönliche Firewall”)

So legen Sie einen der voreingestellten Schutzgrade der Firewall-Funktion von PGPnet fest:

1. Öffnen Sie die Registerkarte **Persönliche Firewall** des Dialogfelds “PGP-Optionen”. (Klicken Sie dazu auf das PGPtray-Schloßsymbol, wählen Sie die Registerkarte **Optionen**, und klicken Sie dann auf die Registerkarte **Persönliche Firewall**.)
2. Klicken Sie auf **Schutzgrad**.

3. Wählen Sie aus der Dropdown-Liste **Schutzgrad** den gewünschten Schutzgrad aus. Zur Wahl stehen die folgenden vordefinierten Schutzgrade:

   - **Keine:** Wählen Sie diesen Schutzgrad, wenn Sie sich sicher sind, daß Ihr System keinen Angriffen ausgesetzt ist. Wenn Sie diese Option wählen, wird Ihr Computer nicht durch die persönliche Firewall von PGPnet geschützt.
   - **Minimal:** Dieser Schutzgrad eignet sich hervorragend für einen typischen Internet- oder Unternehmens-LAN-Benutzer, der einen gewissen grundlegenden Schutz vor üblichen Angriffen benötigt. Wenn Sie diese Option wählen, gelten die folgenden Verkehrseinschränkungen:
     - Eingehender und ausgehender IPsec- und IKE-Verkehr wird zugelassen, so daß Sie sicher über VPN-Verbindungen kommunizieren können.
     - Eingehender ICMP-Verkehr, mit dem Informationen über Ihren Computer abgerufen werden könnten (z. B. Pings oder andere Informationsanforderungen), wird blockiert. Anderer ICMP-Verkehr, einschließlich abgehender ICMP-Verkehr, mit dem Sie Informationen über andere Computer abrufen möchten, wird zugelassen.
     - Anforderungen zum Zugriff auf Windows-Dateien, die aus Ihrem lokalen Teilnetz stammen, werden zugelassen, während solche Anforderungen von außerhalb Ihres lokalen Teilnetzes blockiert werden. Anderer eingehender und abgehender TCP-Verkehr wird zugelassen.
     - Sie können Windows-Domänen, Arbeitsgruppen und Computer in Ihrem lokalen Teilnetz und im Internet durchsuchen.
     - Sämtlicher eingehender und abgehender UDP-Verkehr wird zugelassen.

Client-Schutzgrade

Wenn Ihr Computer als Client arbeitet, müssen Sie einen Client-Schutzgrad auswählen. Das ist der Fall, wenn Ihr Computer in erster Linie zum Anfordern und Abrufen von Daten genutzt wird. Folgende Optionen stehen zur Wahl:

- **Client - Mittel:** Dieser Schutzgrad eignet sich hervorragend für einen Client-Benutzer im Internet oder Unternehmensnetzwerk, der etwas vorsichtiger ist und einen über den Grundschutz hinausgehenden Schutz wünscht. Wenn Sie diese Option wählen, gelten die folgenden Verkehrseinschränkungen:
  - Eingehender und ausgehender IPsec- und IKE-Verkehr werden zugelassen, so daß Sie sicher über VPN-Verbindungen kommunizieren können.
  - Zugelassener ICMP-Verkehr umfaßt abgehende Pings, traceroute und eingehende ICMP-Nachrichten, die für einen effizienten Betrieb des IP-Netzwerks nötig sind. Anderer ICMP-Verkehr wird blockiert.
  - Bestimmter UDP-Verkehr für den Zugriff auf IP-Informationen (wie z. B. die eigene IP-Adresse oder die Netzwerkzeit) wird zugelassen. Verkehr auf höheren UDP-Ports (über 1024) wird ebenfalls zugelassen.
  - Der Zugriff auf Windows-Dateien wird nur zugelassen, wenn Sie sich in Ihrem lokalen Teilnetz bewegen. Außerhalb Ihres lokalen Teilnetzes können Sie sich nicht bewegen, und weder von außerhalb noch von innerhalb Ihres lokalen Teilnetzes kann jemand auf Dateien auf Ihrem Computer zugreifen.
  - Sämtlicher abgehender TCP-Verkehr wird zugelassen, da es sich dabei um einen Client-Schutzgrad handelt und Sie als Client jedermann TCP-Verkehr senden dürfen. Als eingehender TCP-Verkehr wird jedoch nur ftpdata-Verkehr zugelassen, so daß Sie die von Ihnen angeforderten Dateien auch empfangen können.

- **Client - Hoch:** Dieser Schutzgrad eignet sich hervorragend für Internet- oder Unternehmensnetzwerk-Benutzer, die gerade das Ziel von Angriffen sind. Wenn Sie diese Option wählen, wird eingehender und abgehender Verkehr nur in minimalem Umfang zugelassen. Dabei gelten die folgenden Verkehrseinschränkungen:
  - Eingehender und ausgehender IPsec- und IKE-Verkehr wird zugelassen, so daß Sie sicher über VPN-Verbindungen kommunizieren können.
  - ICMP-Verkehr wird nur insoweit zugelassen, wie er für den effizienten Netzwerkbetrieb erforderlich ist. Sowohl eingehende als auch abgehende Pings werden blockiert.
  - UDP-Verkehr wird nur in dem Maße zugelassen, wie er zum Zugriff auf IP-Informationen (wie z. B. die eigene IP-Adresse oder die Netzwerkzeit) erforderlich ist.
  - Der Zugriff auf Windows-Dateien wird nicht zugelassen.
  - Sämtlicher abgehender TCP-Verkehr wird zugelassen. Sämtlicher eingehender TCP-Verkehr wird blockiert.

Server-Schutzgrade

Wenn Ihr Computer als Server arbeitet, müssen Sie einen Server-Schutzgrad auswählen. Das ist der Fall, wenn andere Computer auf Ihren Computer als Datenquelle zugreifen.

HINWEIS: Bei beiden Server-Schutzgraden wird der Zugriff auf Windows-Dateien blockiert. Wenn Sie diese Funktion nutzen möchten, müssen Sie einen benutzerdefinierten Schutzgrad erstellen und die Regel entsprechend bearbeiten. Weitere Informationen zum Erstellen von benutzerdefinierten Schutzgraden und zum Bearbeiten von Regeln finden Sie in “Benutzerdefinierten Schutzgrad erstellen” auf Seite 209.

Folgende Server-Optionen stehen zur Wahl:

- **Server - Mittel:** Dieser Schutzgrad eignet sich hervorragend für einen typischen Server in einem Unternehmensnetzwerk. Wenn Sie diese Option wählen, gelten die folgenden Verkehrseinschränkungen:
  - Eingehender und ausgehender IPsec- und IKE-Verkehr wird zugelassen, so daß Sie sicher über VPN-Verbindungen kommunizieren können.
  - ICMP-Verkehr, der die Kommunikation zwischen einem Server und seinen Clients ermöglicht, wird zugelassen. Sämtlicher anderer ICMP-Verkehr wird blockiert.
  - UDP-Verkehr, der für den Zugriff auf IP-Informationen nötig ist, wird zugelassen. Verkehr auf höheren UDP-Ports (über 1024) wird ebenfalls zugelassen.
  - Sämtlicher eingehender TCP-Verkehr wird zugelassen, da es sich dabei um einen Server-Schutzgrad handelt und der Server TCP-Anfragen von überall her empfangen darf. Als abgehender TCP-Verkehr wird jedoch nur ftpdata- bzw. SMTP-Verkehr zugelassen, so daß Sie auf Datei- oder Mail-Dienstanforderungen antworten können.
- **Server - Hoch:** Dieser Schutzgrad eignet sich hervorragend für Server, die direkt mit dem Internet verbunden und daher einer größeren Angriffsgefahr ausgesetzt sind. Um diesen Schutzgrad so gut wie möglich auszunutzen, empfehlen wir, ihn an die genauen Anforderungen des betreffenden Servers anzupassen. Auf diese Weise können Sie die Firewall so konfigurieren, daß bestimmte Dienste, die der Server unterstützt, zugelassen werden, dabei aber die Anzahl der offenen Ports so gering wie möglich gehalten wird. Weitere Informationen zum Erstellen von benutzerdefinierten Schutzgraden finden Sie in “Benutzerdefinierten Schutzgrad erstellen” auf Seite 209.

  So können Sie beispielsweise auf einem Webserver ICMP-Verkehr sowie HTTP- und HTTPS-Verkehr zulassen, wobei der ICMP-Verkehr an den Anfang der Regelliste gestellt wird und damit die höchste Priorität erhält. Dann können Sie alle Regeln im Regelsatz deaktivieren.

Standardmäßig gelten die folgenden Verkehrseinschränkungen:

- Eingehender und ausgehender IPsec- und IKE-Verkehr wird zugelassen, so daß Sie sicher über VPN-Verbindungen kommunizieren können.
- Bestimmter ICMP-Verkehr, der die Kommunikation zwischen einem Server und seinen Clients ermöglicht, wird zugelassen. Sämtlicher anderer ICMP-Verkehr wird blockiert.
- Bestimmter UDP-Verkehr, der für den Zugriff auf IP-Informationen nötig ist, wird zugelassen. Verkehr auf höheren UDP-Ports (über 1024) wird blockiert.
- Bei TCP-Diensten werden nur die üblicherweise von Servern zur Verfügung gestellten Dienste zugelassen. Sämtlicher anderer TCP-Verkehr wird blockiert. Wenn Ihr Computer einen bestimmten Dienst bereitstellt, können Sie diesen hinzufügen. Sie können aber auch zugelassene Dienste entfernen bzw. deren Status von “Zugelassen” in “Blockiert” ändern.

Spaltenüberschriften der Schutzgrade

Wenn Sie einen vordefinierten Schutzgrad ausgewählt haben, werden im Fenster die Firewall-Regeln (zusammengenommen als “Regelsatz” bezeichnet) in Form von fünf Spalten angezeigt, die im folgenden näher beschrieben werden:

- **Protokoll:** Dieser Spalte lassen sich vier Informationen zur Firewall-Regel entnehmen:
  - Ein Häkchen im Kästchen (☑) zeigt an, daß die Regel aktiv ist.
  - Ein roter Ball ( ) zeigt an, daß der Verkehr, der der Regel entspricht, blockiert wird, während ein grüner Ball ( ) bedeutet, daß der Verkehr, der der Regel entspricht, zugelassen wird.
  - Ein Linkspfeil ( ) steht für eingehenden Verkehr, ein Rechtspfeil ( ) für abgehenden Verkehr und ein Doppelpfeil ( ) steht für Verkehr in beide Richtungen.
  - Das Protokoll, für das die Regel gilt (**ICMP**, **IGMP**, **TCP**, **UDP**, **IPsec ESP**, **IPsec AH** oder **Alle**), wird rechts neben der Spalte angegeben.

- **Service (L):** In dieser Spalte wird der lokale Service angegeben, also der Port auf Ihrem Computer, für den die Regel gilt. Dabei kann es sich um einen einzelnen Service, einen Bereich von Services oder eine Liste von Services handeln. Wenn es sich um einen einzelnen Service handelt, wird unmittelbar hinter dem Servicenamen in Klammern die Portnummer angegeben, die mit dem Service verknüpft ist.

  Zum Beispiel ist der Service für die Datenübertragung (“ftpdata”) normalerweise mit der Portnummer 20 verknüpft. Eine Firewall-Regel, die das Senden von Dateien von Ihrem Computer zuläßt, hat dann in der Spalte “Service (L)” den Eintrag “ftpdata(20)”.

- **Service (R):** In dieser Spalte wird der entfernte Service angegeben, also der Port auf einem entfernten Computer, für den die Regel gilt. Dabei kann es sich um einen einzelnen Service, einen Bereich von Services oder eine Liste von Services handeln. Wenn es sich um einen einzelnen Service handelt, wird unmittelbar hinter dem Servicenamen in Klammern die Portnummer angegeben, die mit dem Service verknüpft ist.

  Wenn wir das Beispiel oben aufgreifen, wird bei einer Firewall-Regel, die das Senden von Dateien von einem entfernten Computer zuläßt, in der Spalte “Service (R)” “ftpdata(20)” aufgeführt.

- **Adresse:** In dieser Spalte werden die Adressen angezeigt, für die die Regel gilt. Bei dem Eintrag kann es sich um eine IP-Adresse, ein Teilnetz oder einen Bereich von IP-Adressen handeln.

- **Ausrufezeichen:** In dieser Spalte wird angegeben, ob eine Übereinstimmung mit den Regelkriterien als Angriff behandelt wird.

4. Klicken Sie auf **OK**. Damit wird der von Ihnen gewählte Schutzgrad eingestellt, und die Registerkarte **Persönliche Firewall** wird geschlossen.

Benutzerdefinierten Schutzgrad erstellen

In PGPnet können Sie einen benutzerdefinierten Schutzgrad erstellen, indem Sie einen der vorhandenen vordefinierten Schutzgrade bearbeiten. Es kann nur ein einziger benutzerdefinierter Schutzgrad erstellt werden. Alle Änderungen, die Sie an Ihrem benutzerdefinierten Schutzgrad vorgenommen haben, überschreiben die vorige Version des benutzerdefinierten Schutzgrads.

Zum Erstellen eines benutzerdefinierten Schutzgrads müssen Sie zunächst einen der vordefinierten Firewall-Schutzgrade auswählen und diesen als Vorlage verwenden. Dann können Sie den Schutzgrad durch eine oder mehrere der folgenden Aktionen anpassen:

- Erstellen Sie eine oder mehrere benutzerdefinierte Regeln, die dem benutzerdefinierten Schutzgrad hinzugefügt werden.
- Bearbeiten Sie die vorhandenen Regeln.
- Entfernen Sie nicht benötigte Regeln aus dem Regelsatz.
- Verschieben Sie Regeln innerhalb des Regelsatzes nach oben oder unten.

So erstellen Sie einen benutzerdefinierten Firewall-Schutzgrad:

1. Öffnen Sie die Registerkarte **Persönliche Firewall** im Dialogfeld "PGP-Optionen". (Klicken Sie dazu auf das PGPtray-Schloßsymbol, wählen Sie **Optionen**, und klicken Sie dann auf die Registerkarte **Persönliche Firewall**.)
2. Wählen Sie aus der Dropdown-Liste der Schutzgrade den vordefinierten Schutzgrad aus, den Sie als Vorlage verwenden möchten. Sie können diesen vorgegebenen Schutzgrad bearbeiten, indem Sie entweder Ihre eigenen benutzerdefinierten Regeln hinzufügen oder indem Sie die Regeln des vorhandenen Regelsatzes ändern.

   Wählen Sie den vordefinierten Schutzgrad aus, der dem Schutzgrad, den Sie definieren möchten, am nächsten kommt. Wenn Ihr Rechner beispielsweise als Client eingesetzt wird und Sie einen benutzerdefinierten Schutzgrad erstellen möchten, der einen hohen Sicherheitsstandard gewährleistet, sollten Sie als Vorlage für Ihren benutzerdefinierten Schutzgrad den Schutzgrad "Client - Hoch" verwenden.
3. Klicken Sie auf **Benutzerdefiniert**. Im unteren Teil der Registerkarte **Persönliche Firewall** werden die Schaltflächen **Neu**, **Bearbeiten**, **Entfernen**, **Nach Oben** und **Nach Unten** angezeigt. Mit Hilfe dieser Schaltflächen können Sie den vorhandenen Regelsatz bearbeiten und auf diese Weise einen benutzerdefinierten Schutzgrad erstellen.

So fügen Sie eine neue Firewall-Regel hinzu:

1. Öffnen Sie die Registerkarte **Persönliche Firewall** im Dialogfeld "PGP-Optionen". (Klicken Sie dazu auf das PGPtray-Schloßsymbol, wählen Sie **Optionen**, und klicken Sie dann auf die Registerkarte **Persönliche Firewall**.)
2. Wählen Sie den vordefinierten Schutzgrad aus, den Sie als Vorlage verwenden möchten.
3. Klicken Sie auf **Benutzerdefiniert**.
4. Klicken Sie auf **Neu**. PGPnet zeigt das Dialogfeld "Firewall-Regel" an (siehe Abbildung 11-2).

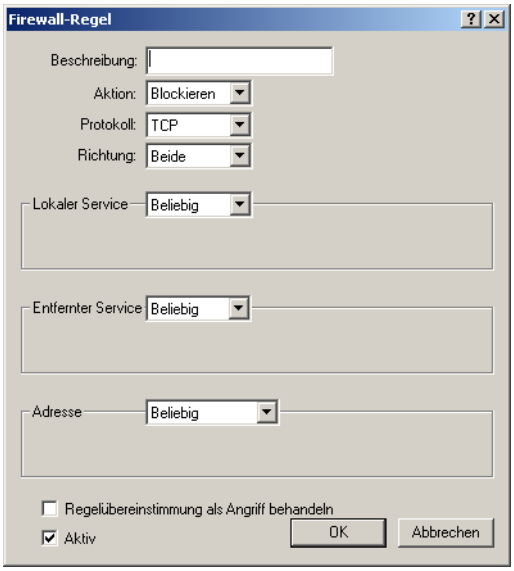


Abbildung 11-2. PGPnet-Dialogfeld "Firewall-Regel"

5. Erstellen Sie eine benutzerdefinierte Firewall-Regel für Ihren benutzerdefinierten Schutzgrad, indem Sie für die Felder im Dialogfeld "Firewall-
Regel" Werte auswählen:
   - **Beschreibung:** Geben Sie eine Beschreibung der Regel in Textform ein.
   - **Aktion:** Legen Sie fest, wie mit dem in der benutzerdefinierten Regel definierten Verkehr verfahren werden soll. Folgende beiden Optionen stehen zur Wahl: **Blockieren** oder **Zulassen**.

- **Protokoll:** Wählen Sie das Protokoll aus, für das die Regel gelten soll: **ICMP**, **IGMP**, **TCP**, **UDP**, **IPsec ESP**, **IPsec AH** oder **Alle**.
- **Richtung:** Wählen Sie die Richtung des Verkehrs aus, für die die Regel gelten soll: **Eingehend**, **Ausgehend** oder **Beide**.
- **Lokaler Service:** Wählen Sie die lokalen Services (Ausgangsportnummern) aus, für die die Regel gelten soll: **Einzeln**, **Bereich**, **Liste** oder **Beliebig**.

HINWEIS: Services können entweder anhand ihres Namens oder anhand der mit ihnen verknüpften Portnummern identifiziert werden. Einen bestimmten Service wählen Sie, indem Sie ihn aus der Liste der Services auswählen oder dessen Portnummer eingeben. HTTP-Services beispielsweise sind meistens mit dem Port 80 verknüpft.

  - Wenn Sie die Option **Einzeln** aktivieren, wählen Sie den gewünschten Service aus dem Dropdown-Menü aus.
  - Wenn Sie die Option **Bereich** aktivieren, geben Sie die erste und die letzte Portnummer des Bereichs ein, den Sie blockieren bzw. zulassen möchten (z. B. 1024 bis 65535).
  - Wenn Sie die Option **Liste** aktivieren, geben Sie die Portnummernwerte ein.
- **Entfernter Service:** Wählen Sie die entfernten Services (Zielportnummern) aus, für die die Regel gelten soll (**Einzeln**, **Bereich**, **Liste** oder **Beliebig**).
  - Wenn Sie die Option **Einzeln** aktivieren, wählen Sie den gewünschten Service aus dem Dropdown-Menü aus.
  - Wenn Sie die Option **Bereich** aktivieren, geben Sie die erste und die letzte Portnummer des Servicebereichs ein, den Sie blockieren bzw. zulassen möchten (z. B. 1024 bis 65535).
  - Wenn Sie die Option **Liste** aktivieren, geben Sie die Portnummernwerte ein.

- **Adresse:** Wählen Sie die entfernten Adressen aus, für die die Regel gelten soll (**Einzeln**, **Teilnetz**, **Lokales Teilnetz**, **Bereich** oder **Beliebig**).
  - Wenn Sie die Option **Einzeln** aktiviert haben, geben Sie im Feld **Adresse** die IP-Adresse des Systems ein, das Sie blockieren bzw. zulassen möchten. Verwenden Sie dabei folgendes Format: nnn.nnn.nnn.nnn.
  - Wenn Sie die Option **Teilnetz** aktiviert haben, geben Sie in den Feldern **Adresse** und **Maske** die IP-Adresse und Maske des Teilnetzes ein, das Sie blockieren bzw. zulassen möchten. Verwenden Sie dabei folgendes Format: nnn.nnn.nnn.nnn.
  - Wenn Sie die Option **Bereich** aktiviert haben, geben Sie in den Feldern **Von** (erste Adresse) und **Bis** (letzte Adresse) die erste und die letzte IP-Adresse ein.

6. Um festzulegen, daß die Übereinstimmung mit einer Regel als Angriff betrachtet werden soll, aktivieren Sie die Option **Regelübereinstimmung als Angriff behandeln**. Wenn PGPnet Pakete erkennt, die dieser Regel entsprechen, betrachtet das Programm die entsprechende Kommunikation als Angriff und verhält sich entsprechend den Festlegungen auf der Registerkarte **Persönliches IDS**. Wenn Sie diese Option aktiviert haben, wird in der letzten Spalte der Registerkarte **Persönliche Firewall** ein Ausrufezeichen angezeigt.
7. Zur Aktivierung der Regel klicken Sie auf **Aktiv**.
8. Klicken Sie auf **OK**, um das Dialogfeld “Firewall-Regel” zu schließen. Die von Ihnen erstellte neue Regel wird in der obersten Position der Regelliste auf der Registerkarte **Persönliche Firewall** angezeigt. Dies ist der Regelsatz für Ihren benutzerdefinierten Schutzgrad.
9. Klicken Sie auf **OK**, um die Registerkarte **Persönliche Firewall** zu schließen. Damit wird der von Ihnen erstellte benutzerdefinierte Schutzgrad gespeichert und als aktiver Schutzgrad festgelegt.

WARNUNG: Wenn Sie die Registerkarte **Persönliche Firewall** schließen, indem Sie auf das **X** in der rechten oberen Ecke der Registerkarte klicken, wird Ihr benutzerdefinierter Schutzgrad nicht gespeichert.

So bearbeiten Sie eine vorhandene Regel:

1. Öffnen Sie die Registerkarte **Persönliche Firewall** im Dialogfeld "PGP-Optionen". (Klicken Sie dazu auf das PGPtray-Schloßsymbol, wählen Sie **Optionen**, und klicken Sie dann auf die Registerkarte **Persönliche Firewall**.)
2. Vergewissern Sie sich, daß die Option **Benutzerdefiniert** aktiviert ist.
3. Wählen Sie die Firewall-Regel aus, die Sie bearbeiten möchten.
4. Klicken Sie auf **Bearbeiten**. PGPnet zeigt das Dialogfeld "Firewall-Regel" an.
5. Nehmen Sie die gewünschten Änderungen an der ausgewählten Regel vor.
6. Klicken Sie im Dialogfeld "Firewall-Regel" auf **OK**.
7. Klicken Sie auf **OK**, um die Registerkarte **Persönliche Firewall** zu schließen und den benutzerdefinierten Schutzgrad zu aktivieren.

> **WARNUNG:** Wenn Sie die Registerkarte **Persönliche Firewall** schließen, indem Sie auf das **X** in der rechten oberen Ecke der Registerkarte klicken, werden die Änderungen, die Sie an Ihrem benutzerdefinierten Schutzgrad vorgenommen haben, nicht gespeichert.

So entfernen Sie eine Regel:

1. Öffnen Sie die Registerkarte **Persönliche Firewall** im Dialogfeld "PGP-Optionen". (Klicken Sie dazu auf das PGPtray-Schloßsymbol, wählen Sie **Optionen**, und klicken Sie dann auf die Registerkarte **Persönliche Firewall**.)
2. Vergewissern Sie sich, daß die Option **Benutzerdefiniert** aktiviert ist.
3. Wählen Sie die Firewall-Regel aus, die Sie entfernen möchten.
4. Klicken Sie auf **Entfernen**.
5. Klicken Sie auf **OK**, um die Registerkarte **Persönliche Firewall** zu schließen und den benutzerdefinierten Schutzgrad zu aktivieren.

So ändern Sie die Priorität einer Regel:

Die Regeln erhalten je nach ihrer Position innerhalb der Regelliste eine bestimmte Priorität. Je weiter oben die Regel in der Liste steht, desto höher ist deren Priorität.

1. Öffnen Sie die Registerkarte **Persönliche Firewall** im Dialogfeld "PGP-Optionen". (Klicken Sie dazu auf das PGPtray-Schloßsymbol, wählen Sie **Optionen**, und klicken Sie dann auf die Registerkarte **Persönliche Firewall**.)
2. Vergewissern Sie sich, daß die Option **Benutzerdefiniert** aktiviert ist.
3. Wählen Sie die Firewall-Regel aus, deren Priorität Sie ändern möchten.
4. Um eine Regel innerhalb der Liste nach unten zu verschieben, müssen Sie die Regel auswählen und anschließend auf **Nach Unten** klicken. Um eine Regel in der Liste nach oben zu verschieben, müssen Sie die Regel auswählen und anschließend auf **Nach Oben** klicken.
5. Klicken Sie auf **OK**, um die Registerkarte **Persönliche Firewall** zu schließen und den benutzerdefinierten Schutzgrad zu aktivieren.

Das persönliche Angrifferkennungssystem (IDS) in PGPnet konfigurieren

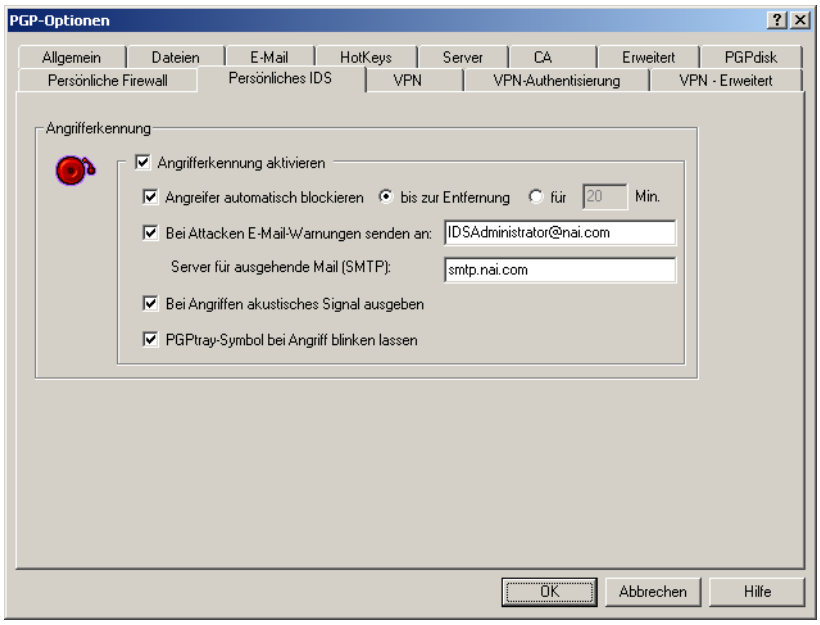


Abbildung 11-3. Dialogfeld “PGP-Optionen” (Registerkarte “Persönliches IDS”)

Das in PGPnet enthaltene Angrifferkennungssystem (Intrusion Detection System, IDS) ist für die Benutzer gedacht, die auch von der PGPnet-Funktion “Persönliche Firewall” geschützt werden sollen, also kleine Büros ohne eine Unternehmens-Firewall, Benutzer in Unternehmen, die außerhalb der Unternehmens-Firewall arbeiten und Benutzer im Home Office-Bereich. Diese Funktion schützt isolierte Rechner vor verschiedensten Angriffen (z. B. Port-Scans, IP-Spoofing und SYN-Flood).

Diesen Angriffen können alle ungeschützten Rechner zum Opfer fallen. So können Angreifer beispielsweise durch einen TCP-Port-Scan herausfinden, welche Dienste auf Ihrem Rechner aktiv sind. Danach können sie versuchen, eine Verbindung zu diesen Services aufzubauen und Ihren Rechner anzugreifen. Wenn der Angreifer entdeckt, daß auf Ihrem Rechner ein TELNET-, FTP- oder Web-Server läuft, testet er nacheinander alle Ports Ihres Rechners von 1 bis 65535, bis er einen offenen Port gefunden hat, über den sich die Verbindung aufbauen läßt.

Im Gegensatz zu anderen Angrifferkennungs-Tools läßt sich die leistungsstarke PGPnet-Funktion einfach konfigurieren und aktivieren. Beim IDS von PGPnet müssen sich die Benutzer nicht erst umfangreiches Wissen über mögliche Angriffe aneignen, um dann ihre eigene Verteidigungsstrategie gegen Eindringlinge entwickeln zu können. Statt dessen hat unser Entwicklungsteam ein Tool geschaffen, das durch einfaches Klicken auf eine Schaltfläche aktiviert werden kann und selbständig alle üblichen Angriffstypen sowie bereits verdächtige Aktivitäten erkennt.

Die PGPnet-Funktion “IDS” sucht dabei nach bestimmten Verkehrsmustern, die von Angreifern verwendet werden. PGPnet überprüft jedes einzelne Datenpaket, das in Ihrem Rechner ankommt, um verdächtige Verkehrsmuster oder typische Angriffsmuster aufzuspüren. Wenn PGPnet beispielsweise Telnet-Pakete erkennt, analysiert die Software diese Pakete hinsichtlich verdächtiger Verkehrsmuster; der Telnet-Verkehr wird mit bekannten Angriffsmustern verglichen. Wenn PGPnet dabei Datenpakete entdeckt, die einem bekannten Angriffsmuster entsprechen, erzeugt die Software ein Ereignis und verständigt Sie über die potentielle Sicherheitsverletzung.

Entdeckt PGPnet bei aktivierter Angrifferkennungsfunktion einen Angriff, kann der gesamte zukünftige Verkehr von der IP-Adresse des verdächtigen Rechners blockiert werden, und zwar entweder auf unbestimmte Zeit oder für eine vom Benutzer festgelegte Zeitdauer. Sie können die Funktion auch so einrichten, daß beim Erkennen eines Angriffs eine E-Mail an einen bestimmten Empfänger gesendet wird oder / und ein akustisches Warnsignal ertönt. In einer solchen E-Mail können mehrere Benachrichtigungen enthalten sein. Eine diesbezügliche E-Mail könnte beispielsweise wie folgt lauten: “SYN Flood-Angriff entdeckt bei 10.23.140.33 am Montag, 24. Juli 2001, 16:15:19”.

Wenn ein Angriff entdeckt wird, wird das PGPtray-Symbol mit einem Ausrufezeichen versehen, das anfängt zu blinken. Klicken Sie in einem solchen Fall auf das PGPtray-Symbol, um die Registerkarte **Einbrecher** (sofern die automatische Blockierung aktiviert ist) bzw. die Registerkarte **Protokoll** (sofern die automatische Blockierung nicht aktiviert ist) aufzurufen. Weitere Angriffe, die von den auf der Registerkarte **Einbrecher** (siehe Abbildung 11-4 auf Seite 218) aufgeführten Hosts ausgehen, werden nicht mehr gemeldet.

Wenn die Angrifferkennung aktiviert ist, wird der gesamte Verkehr vom Angrifferkennungssystem geprüft.

HINWEIS: Da PGPnet Pakete analysiert und nach Paketmustern sucht, die typisch für bestimmte Angriffsarten sind, kann diese Funktion zu einer sehr geringfügigen Verringerung der Arbeitsgeschwindigkeit Ihres Rechners führen.

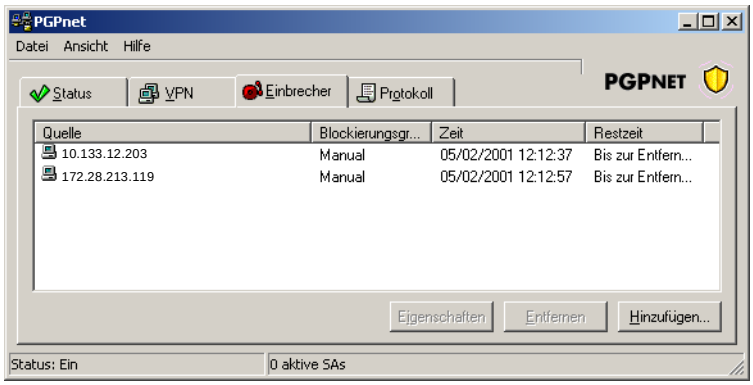


Abbildung 11-4. Dialogfeld “PGPnet” (Registerkarte “Einbrecher” – blockierte Hosts)

So konfigurieren Sie die PGPnet-Funktion “Persönliche Angrifferkennung”:

1. Öffnen Sie die Registerkarte **Persönliches IDS** im Dialogfeld “PGP-Optionen”. (Klicken Sie dazu auf das PGPtray-Schloßsymbol, wählen Sie **Optionen**, und klicken Sie dann auf die Registerkarte **Persönliches IDS**.)

2. Zur Aktivierung der PGPnet-Angrifferkennungsfunktion klicken Sie auf **Angrifferkennung aktivieren** (das Feld wird dabei mit einem Häkchen versehen). Zum Deaktivieren der PGPnet-Angrifferkennungsfunktion klicken Sie auf **Angrifferkennung aktivieren** (das Häkchen wird dabei aus dem Feld entfernt).

3. Um den von der IP-Adresse eines Angreifers ausgehenden Verkehr zu blockieren, klicken Sie auf **Angreifer automatisch blockieren**. Sie können festlegen, wie lange PGPnet den von der IP-Adresse des Angreifers ausgehenden Verkehr blockieren soll:

   - Wenn der Verkehr so lange blockiert werden soll, bis Sie den Host aus der Registerkarte **Einbrecher** entfernen, klicken Sie auf **Bis zur Entfernung**.

   - Wenn der von der IP-Adresse des Angreifers ausgehende Verkehr für eine bestimmte Anzahl von Minuten blockiert werden soll, klicken Sie auf **für [ ] Min.**, und geben Sie die Anzahl der Minuten ein.

4. Wenn bei einem Angriff eine Benachrichtigungs-E-Mail gesendet werden soll, klicken Sie auf **Bei Attacken E-Mail-Warnungen senden an:**, und geben Sie die E-Mail-Adresse ein. Wenn PGPnet den jeweiligen Mail-Server identifizieren kann, zeigt die Software im Feld **Server für ausgehende Mail (SMTP)** die entsprechenden Daten an. Wenn dieses Feld leer ist, geben Sie den Namen des Servers ein, über den die E-Mail-Warnungen gesendet werden sollen. Falls Sie den Namen des Servers nicht kennen, überprüfen Sie die Einstellungen Ihres E-Mail-Clients.

5. Wenn im Falle eines Angriffs eine akustische Warnung ausgegeben werden soll, klicken Sie auf **Bei Angriffen akustisches Signal ausgeben**.

6. Wenn bei einem Angriff das PGPtray-Symbol blinken soll, klicken Sie auf **PGPtray-Symbol bei Angriff blinken lassen**.

7. Klicken Sie auf **OK**.

Die PGPnet-Funktion “VPN” konfigurieren 12

In diesem Kapitel wird beschrieben, wie Sie die PGPnet-Funktion “VPN” konfigurieren können. Wenn Sie Benutzer innerhalb einer Unternehmensumgebung sind, könnte Ihr PGP- bzw. PGPnet-Administrator das Konfigurieren dieser Funktion bereits für Sie vorgenommen haben.

Um die PGPnet-Funktion “VPN” nutzen zu können, müssen Sie folgende Schritte ausführen:

1. Starten Sie PGPnet (siehe “Schritt 1. PGPnet-Programm starten” auf Seite 222).
2. Wählen Sie Ihren Authentisierungsschlüssel bzw. Ihr Authentisierungszertifikat aus (siehe “Schritt 2. Authentisierungsschlüssel bzw. -zertifikat auswählen” auf Seite 222).
3. Importieren Sie eine vorhandene Hostliste (siehe “Schritt 3a. Hostliste importieren” auf Seite 223), oder fügen Sie PGPnet Hosts hinzu (siehe “Schritt 3b. Host, Teilnetz oder Gateway hinzufügen” auf Seite 224).
4. Richten Sie SAs (Security Associations, Sicherheitsverbindungen) ein (siehe “Schritt 4. SA einrichten” auf Seite 224).

Die weiteren Themen, die in diesem Kapitel behandelt werden, sind in der folgenden Tabelle aufgeführt.

Thema:	Siehe:
Verwenden des Assistenten für das Hinzufügen von Hosts	“Assistenten für das Hinzufügen von Hosts verwenden” auf Seite 226
Verwenden des Expert-Modus	“Expert-Modus: Hosts, Gateways oder Teilnetze ohne Assistenten hinzufügen” auf Seite 234
Verwenden der Funktion “DNS-Lookup”	“DNS-Suche: IP-Adresse eines Hosts suchen” auf Seite 236
entferntes Authentisieren – Vorlage eines bestimmten Schlüssels oder eines bestimmten Zertifikats vom Host fordern	“Entfernte Authentisierung” auf Seite 237

Thema:	Siehe:
Gemeinsames Geheimnis	“Gemeinsames Geheimnis” auf Seite 237
Verwenden der Funktionen “Abrufen der virtuellen Identität” und “Exklusiver Gateway”	“Die Funktionen “Abrufen der virtuellen Identität” und “Exklusiver Gateway”” auf Seite 239

Schritt 1. PGPnet-Programm starten

PGPnet läßt sich mit zwei Methoden starten:

- Wählen Sie **Start—>Programme—>PGP—>PGPnet**.

  oder

- Starten Sie PGPnet über das PGPtray-Symbol im Systemfeld der Windows-Taskleiste (**PGPtray—>PGPnet—>Status**, **VPN**, **Einbrecher oder Protokoll**).

Schritt 2. Authentisierungsschlüssel bzw. -zertifikat auswählen

Bevor Sie PGPnet verwenden, müssen Sie den Schlüssel und/oder das X.509-Zertifikat auswählen, den bzw. das Sie zur Authentisierung verwenden möchten. Falls Sie kein vorhandenes Schlüsselpaar oder X.509-Zertifikat besitzen, lesen Sie unter “Schlüssel erstellen und austauschen” auf Seite 41 nach.

So wählen Sie Ihren Authentisierungsschlüssel oder/und Ihr Zertifikat aus:

1. Klicken Sie auf das Menü **Ansicht** im PGPnet-Fenster, und wählen Sie **Optionen**.
2. Klicken Sie auf die Registerkarte **VPN-Authentisierung**.
3. Wählen Sie den Schlüssel und/oder das Zertifikat aus, der bzw. das zur Authentisierung verwendet werden soll. (Klicken Sie dazu auf **Schlüssel auswählen** oder auf **Zertifikat auswählen**.) Beachten Sie, daß der Schlüssel oder das Zertifikat Teil eines Schlüsselpaars sein muß und Sie über den privaten Schlüssel verfügen müssen.
4. Klicken Sie auf **OK**. In einem Dialogfeld werden Sie aufgefordert, die Paßphrase für den ausgewählten Schlüssel einzugeben.
5. Geben Sie die Paßphrase ein, und klicken Sie auf **OK**.

WICHTIG: Wenn Sie eine VPN-Verbindung mit einem anderen PGPnet-Host herstellen und PGPkeys zur Authentisierung verwenden, muß von beiden derselbe PGP-Schlüsseltyp verwendet werden. Wird an einem Ende der Verbindung ein RSA-Schlüssel und am anderen ein DH / DSS-Schlüssel verwendet, kann keine SA abgestimmt werden.

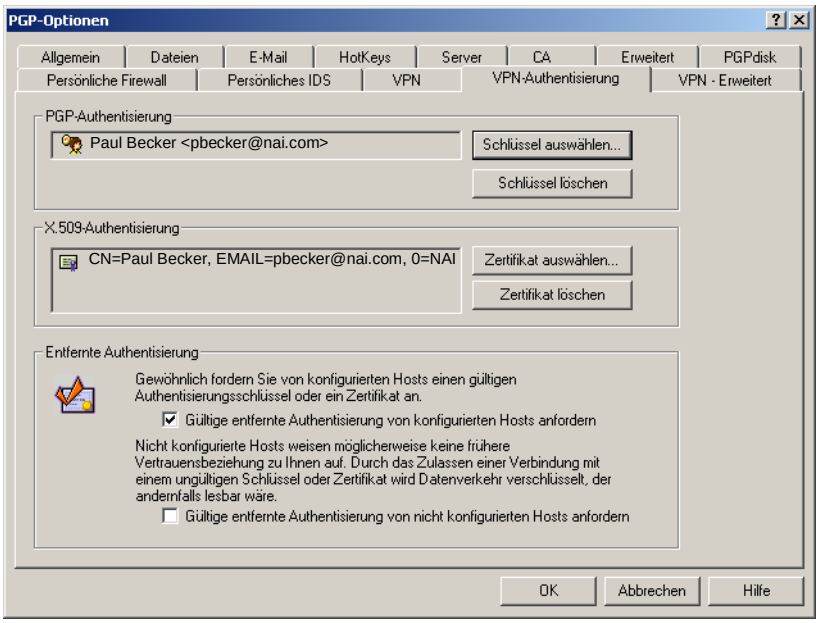


Abbildung 12-1. Registerkarte “VPN-Authentisierung”

Schritt 3a. Hostliste importieren

PGPnet verfügt über eine Funktion zum Importieren einer vorhandenen Hostliste in die PGPnet-Datenbank. Das erspart Ihnen das manuelle Hinzufügen der Hosts zur Hostliste. Bei der Hostliste muß es sich jedoch um eine zuvor aus PGPnet exportierte Liste handeln.

So importieren Sie eine Hostliste:

1. Wählen Sie im PGPnet-Menü **Datei** den Befehl **Hosts importieren**. Daraufhin wird das Dialogfeld “Datei mit Hostliste auswählen” angezeigt.
2. Wählen Sie die Datei aus, die die Hostliste enthält. Die Hosts aus der Datei mit der Hostliste werden auf der Registerkarte**VPN** angezeigt.

Schritt 3b. Host, Teilnetz oder Gateway hinzufügen

HINWEIS: Dieser Schritt ist nicht erforderlich, wenn Sie eine Hostliste importiert haben.

So fügen Sie einen Host, ein Teilnetz oder einen Gateway hinzu:

1. Klicken Sie auf die Registerkarte **VPN** im PGPnet-Fenster.
2. Klicken Sie auf **Hinzufügen**.
3. Befolgen Sie die Anweisungen auf der Registerkarte des **Assistenten für das Hinzufügen von Hosts**. (Weitere Informationen dazu, wie Sie mit Hilfe des **Assistenten für das Hinzufügen von Hosts** Hosts hinzufügen können, finden Sie im Abschnitt “Assistenten für das Hinzufügen von Hosts verwenden” auf Seite 226.)

Schritt 4. SA einrichten

Zur Kommunikation mit den von Ihnen in Schritt 3 hinzugefügten Hosts, Teilnetzen und Gateways müssen Sie Sicherheitsverbindungen (Security Associations, SAs) erstellen.

So richten Sie eine SA mit einem anderen Host ein:

1. Vergewissern Sie sich, daß beide Systeme über eine Netzwerkverbindung verfügen.
2. Installieren Sie PGPnet auf beiden Systemen.
3. Starten Sie nach der Installation von PGPnet beide Systeme neu.

4. Beachten Sie dabei folgende Punkte:

   - Wenn Sie zur Authentisierung PGP-Schlüssel oder X.509-Zertifikate verwenden, müssen Sie gewährleisten, daß für jedes System auf der Registerkarte **VPN-Authentisierung** ein Schlüssel bzw. ein Zertifikat für die Authentisierung festgelegt ist (wählen Sie dazu **Ansicht—>Optionen—>VPN-Authentisierung**).

   - Wenn Sie PGP-Schlüssel zur Authentisierung verwenden, müssen Sie sich vergewissern, daß die öffentlichen Schlüssel, die jedes System zur Authentisierung nutzt, ausgetauscht, unterschrieben und überprüft wurden.

   - Wenn Sie zur Authentisierung X.509-Zertifikate verwenden, müssen Sie sicherstellen, daß die Root-CA für das X.509-Zertifikat der entfernten Seite vorhanden, unterschrieben und auf beiden Systemen 100%ig autorisiert ist.

   - Wenn Sie zur Authentisierung PGP-Schlüssel oder X.509-Zertifikate verwenden, muß zumindest ein Benutzer einen Eintrag in der PGPnet-Hostliste für das andere System erstellen (verwenden Sie dazu die Schaltfläche **Hinzufügen** auf der Registerkarte **VPN**). Wenn der Modus **Versuchen** eingestellt ist (Registerkarte **VPN**), können Sie mit der Kommunikation beginnen.

   - Wenn die Authentisierung durch eine *gemeinsame geheime Paßphrase* erfolgt, müssen beide Benutzer einen Eintrag in der PGPnet-Hostliste für das jeweils andere System erstellen und sich auf eine gemeinsame geheime Paßphrase einigen. Die Paßphrase kann ein Wort oder eine Wortgruppe sein. Das bedeutet, daß beide Benutzer sich auf die Kommunikationsbedingungen, also das Verschlüsselungsverfahren usw., geeinigt haben.

5. Wählen Sie den Hosteintrag auf der Registerkarte **VPN** aus, und klicken Sie anschließend auf **Verbinden**. Falls der Verbindungsaufbau erfolgreich war, wird in der Spalte **SA** ein grüner Kreis angezeigt.

Assistenten für das Hinzufügen von Hosts verwenden

HINWEIS: Falls Sie zu den erfahrenen Benutzern zählen, ziehen Sie “Expert-Modus: Hosts, Gateways oder Teilnetze ohne Assistenten hinzufügen” auf Seite 234 zu Rate.

Wenn Sie in einer Unternehmensumgebung arbeiten, für deren Betreuung ein PGPnet-Administrator zuständig ist, wurden wahrscheinlich viele der Hosts, Teilnetze und Gateways, mit denen Sie kommunizieren, bereits vorkonfiguriert. Für alle vorkonfigurierten Hosts, Teilnetze und Gateways gibt es einen Eintrag in der Hostliste von PGPnet. Wenn Sie der Hostliste zusätzliche Einträge hinzufügen möchten, stehen Ihnen dazu der Assistent zum **Hinzufügen von Hosts** bzw. das Dialogfeld “Host/Gateway” zur Verfügung.

Wenn Sie keinen PGPnet-Administrator haben, oder bei der Installierung von PGPnet keine Hosts, Teilnetze oder Gateways konfiguriert sind, wird **der Assistent zum Hinzufügen von Hosts** automatisch beim ersten Start von PGPnet gestartet. Mit diesem Assistenten können Sie die notwendigen Hosts, Teilnetze und Gateways hinzufügen. Welche Hosts, Teilnetze und Gateways vorhanden sind, wird auf der Registerkarte **VPN** angezeigt.

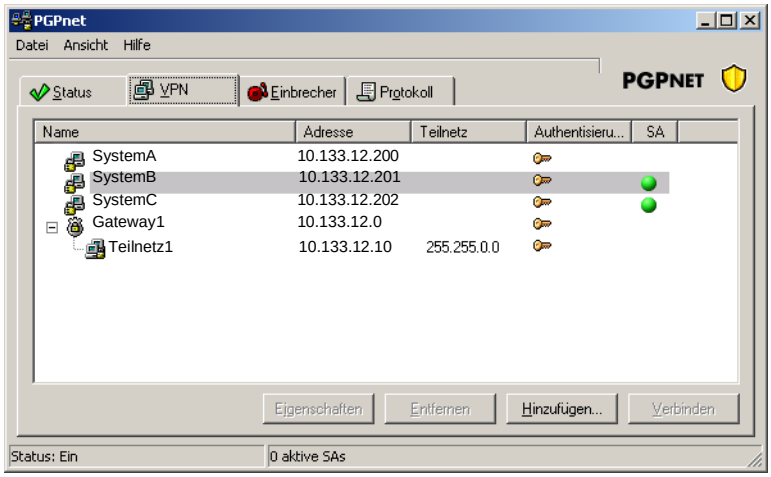


Abbildung 12-2. Registerkarte “VPN”

Benötigte Informationen

Im folgenden Abschnitt sind die Informationen genannt, die Sie zum Hinzufügen eines Hosts, eines Teilnetzes oder Gateways benötigen.

Ziel:	Benötigte Informationen:
Sicheren Host hinzufügen	Host-Domäne oder IP-Adresse
Teilnetz hinzufügen	IP-Adresse und Teilnetzmaske
Gateway hinzufügen	Host-Domäne oder IP-Adresse
Exklusiven Gateway hinzufügen	Host-Domäne oder IP-Adresse
Host hinter konfiguriertem Gateway hinzufügen	Host-Domäne oder IP-Adresse
Teilnetz hinter konfiguriertem Gateway hinzufügen	IP-Adresse und Teilnetzmaske

HINWEIS: Sie können einen sicheren Gateway und einen sicheren Host (der nicht hinter einem Gateway liegt) mit derselben IP-Adresse haben. In diesem Fall wird der Hosteintrag automatisch auf **Manuelle Verbindung** gesetzt (d. h., Sie müssen, um die Verbindung zum Host aufzubauen, im PGPnet-Menü von PGPtray auf den Host oder auf **Verbinden** auf der Registerkarte **VPN** klicken).

Host hinzufügen

Im folgenden Abschnitt wird beschrieben, wie der Hostliste ein Hosteintrag hinzugefügt wird und wie Sie einen Host hinter einem bereits konfigurierten Gateway oder Teilnetz hinzufügen können.

Dabei wird davon ausgegangen, daß Sie dazu den **Assistenten für das Hinzufügen von Hosts** verwenden. Wenn in Schritt 2 das Dialogfeld “Host / Gateway” angezeigt wird, klicken Sie auf **Assistent verwenden** (unten links), um zum Assistenten zurückzukehren.

1. Klicken Sie im Hauptfenster von PGPnet auf die Registerkarte **VPN**.

   Wenn Sie einen Host hinter einem bereits konfigurierten Gateway hinzufügen möchten, wählen Sie den konfigurierten Gateway.

   Wenn Sie einen Host hinter einem bereits konfigurierten Teilnetz hinzufügen möchten, wählen Sie das konfigurierte Teilnetz.

2. Klicken Sie auf **Hinzufügen**. PGPnet zeigt den **Assistenten zum Hinzufügen von Hosts** an. Lesen Sie sich die Informationen auf dem ersten Bildschirm durch, und klicken Sie auf **Weiter**.

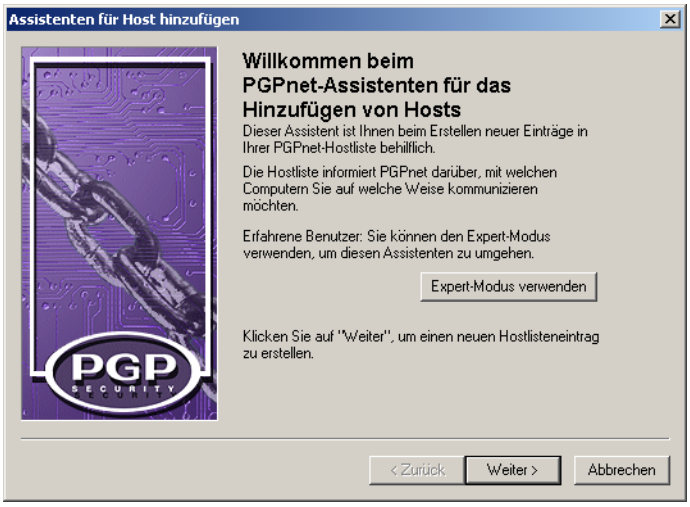


Abbildung 12-3. Assistent zum Hinzufügen von Hosts

Wenn Sie einen Host oder einen Host hinter einem konfigurierten Teilnetz hinzufügen möchten, fahren Sie mit Schritt 3 fort.

Wenn Sie einen Host hinter einem konfigurierten Gateway hinzufügen möchten, fragt der Assistent, ob ein neuer Hosteintrag für einen Computer oder ein Teilnetz erstellt werden soll, auf den bzw. das über den ausgewählten Gateway zugegriffen wird.

Wenn Sie einen Eintrag für einen Host hinter dem Gateway erstellen möchten, wählen Sie **Ja**, und klicken dann auf **Weiter**.

Sie werden aufgefordert, den zu konfigurierenden Kommunikationstyp auszuwählen. Wählen Sie **Host**, und klicken Sie anschließend auf **Weiter**.

Fahren Sie mit Schritt 4 fort.

3. Im Assistenten müssen Sie angeben, ob Sie einen Host, ein Teilnetz oder einen Gateway hinzufügen möchten. Klicken Sie auf **Host** und anschließend auf **Weiter**.

4. Wählen Sie, ob Sie die sichere Kommunikation erzwingen oder die unsichere Kommunikation zulassen möchten. Aktivieren Sie die gewünschte Option, und klicken Sie dann auf **Weiter**.

5. Geben Sie einen aussagekräftigen Namen für den Computer ein, mit dem Sie die Kommunikation durchführen möchten. Klicken Sie auf **Weiter**.

6. Geben Sie entweder den Host-Domänennamen oder die IP-Adresse für den Host ein. Klicken Sie auf **Weiter**. Wenn Sie einen Host-Domänennamen eingeben, sucht der Assistent nach Ihrem Eintrag. Falls der Assistent Ihren Eintrag nicht finden kann, klicken Sie auf **Zurück**, um zum vorigen Bildschirm zurückzukehren, und geben Sie erneut den Namen oder die IP-Adresse ein.

   Wenn Sie sich entschieden haben, unsichere Kommunikation zuzulassen, wird Ihr Eintrag in die Hostliste aufgenommen. Wenn Sie festgelegt haben, daß sichere Kommunikation erzwungen werden soll, fahren Sie bitte mit dem folgenden Schritt fort.

7. Geben Sie an, ob die Kommunikation mit diesem Rechner über einen öffentlichen Schlüssel verschlüsselt oder per gemeinsamer geheimer Paßphrase geschützt werden soll. Klicken Sie auf **Weiter**. Wenn Sie sich für die Sicherung der Kommunikation durch eine gemeinsame geheime Paßphrase entschieden haben, geben Sie diese ein. Beachten Sie, daß auf beiden Hosts dieselbe gemeinsame geheime Paßphrase konfiguriert sein muß. Klicken Sie auf **Weiter**.

8. Legen Sie fest, wie die Verbindung zu diesem Host aufgebaut werden soll: **Automatisch** (immer dann, wenn Verkehr an diesen Host gesendet wird bzw. von diesem empfangen wird) oder **Manuell** (durch Klicken auf **Verbinden** auf der Registerkarte **Hosts**). Den Verbindungsmodus für diesen Hosteintrag können Sie durch Klicken auf die Schaltfläche **Eigenschaften** auf der Registerkarte **VPN** jederzeit ändern.

9. PGPnet fügt Ihren Eintrag der Hostliste hinzu.

Teilnetz oder Gateway hinzufügen

Im folgenden Abschnitt wird beschrieben, wie ein Teilnetz oder ein Gateway hinzugefügt wird, und wie Sie ein Teilnetz hinter einem bereits konfigurierten Gateway hinzufügen können.

Dabei wird davon ausgegangen, daß Sie dazu den **Assistenten für das Hinzufügen von Hosts** verwenden. Wenn in Schritt 2 das Dialogfeld “Host / Gateway” angezeigt wird, klicken Sie auf **Assistent verwenden** (unten links), um zum Assistenten zurückzukehren.

1. Klicken Sie im Hauptfenster von PGPnet auf die Registerkarte **VPN**.

   Wenn Sie ein Teilnetz hinter einem bereits konfigurierten Gateway hinzufügen möchten, wählen Sie den konfigurierten Gateway.

2. Klicken Sie auf **Hinzufügen**. PGPnet zeigt den **Assistenten zum Hinzufügen von Hosts** an. Lesen Sie sich die Informationen auf dem ersten Bildschirm durch, und klicken Sie auf **Weiter**.

   Wenn Sie ein Teilnetz hinter einem bereits konfigurierten Gateway hinzufügen möchten, fahren Sie mit Schritt 3 fort. Ist dies nicht der Fall, fahren Sie mit Schritt 4 fort.

3. Bei der Kommunikation mit einem Computer oder Teilnetz kann der Computer bzw. das Teilnetz entweder direkt zugänglich sein oder sich auf der anderen Seite eines sicheren Gateways (z. B. einer Firewall) befinden.

   Wenn Sie einen Eintrag für ein Teilnetz hinter dem Gateway erstellen möchten, wählen Sie **Ja**. Klicken Sie dann auf **Weiter**.

4. Der Assistent fragt, ob Sie einen Host oder ein Teilnetz (bzw. einen Host, ein Teilnetz oder einen Gateway) hinzufügen möchten. Klicken Sie auf **Teilnetz** oder **Gateway** und anschließend auf **Weiter**.

   Wenn Sie ein Teilnetz hinzufügen möchten, fahren Sie bitte mit Schritt 5 fort.

   Wenn Sie einen Gateway hinzufügen möchten, fahren Sie bitte mit Schritt 6 fort.

5. Wählen Sie, ob Sie die sichere Kommunikation erzwingen oder die unsichere Kommunikation zulassen möchten. Klicken Sie auf Ihre Auswahl und dann auf **Weiter**.

6. Geben Sie für den Computer, mit dem Sie kommunizieren möchten, einen aussagekräftigen Namen ein. Klicken Sie auf **Weiter**.

7. Wenn Sie ein Teilnetz hinzufügen, müssen Sie die IP-Adresse für das Teilnetz eingeben. Wenn Sie einen Gateway eingeben, müssen Sie den Host-Domänennamen bzw. die IP-Adresse für den Gateway eingeben.

8. Geben Sie an, ob die Kommunikation mit diesem Rechner über einen öffentlichen Schlüssel verschlüsselt oder per gemeinsamer geheimer Paßphrase geschützt werden soll. Klicken Sie auf **Weiter**. Wenn Sie sich für die Sicherung der Kommunikation durch eine gemeinsame geheime Paßphrase entschieden haben, geben Sie diese ein. Beachten Sie, daß auf beiden Hosts dieselbe gemeinsame geheime Paßphrase konfiguriert sein muß. Klicken Sie auf **Weiter**.

   Wenn Sie ein Teilnetz hinzufügen möchten, fahren Sie mit Schritt 9 fort.

   Wenn Sie einen Gateway hinzufügen möchten, fahren Sie mit Schritt 10 fort.

WARNUNG: Im Gegensatz zu herkömmlichen PGP-Paßphrasen werden gemeinsame geheime Paßphrasen unverschlüsselt auf dem Computer gespeichert. Dies stellt ein mögliches Sicherheitsrisiko dar.

9. Legen Sie fest, wie der Verbindungsaufbau zu diesem Host erfolgen soll:

   - **Automatisch verbinden:** Wählen Sie diese Option, wenn PGPnet bei jeder Paketsendung an den Hosteintrag automatisch die Verbindung herstellen soll.
   - **Manuelle Verbindung anfordern:** Wählen Sie diese Option, wenn Sie Ihren Computer an mehreren Standorten einsetzen (z. B. als Firmenmitarbeiter, der seinen Laptop sowohl im Büro als auch zu Hause nutzt). Diese Funktion ermöglicht eine sichere Kommunikation mit denselben Hosts von beiden Seiten eines Firmen-Gateways unter Nutzung eines der beiden Adapter Ihres Computers. Zum manuellen Verbindungsaufbau verwenden Sie die Schaltfläche **Verbinden** auf der Registerkarte **VPN**.

     Wenn Sie ein Teilnetz bzw. ein Teilnetz hinter einem Gateway hinzufügen, fügt PGPnet den Eintrag in die Hostliste ein.

10. **Abrufen der virtuellen Identität für diesen Gateway aktivieren.** Diese Option wird angezeigt, wenn Sie einen Eintrag für einen Gateway hinzufügen.

HINWEIS: Die PGPnet-Funktion “Virtuelle Identität” basiert auf dem von der IPsec-Arbeitsgruppe der IETF entworfenen “config-mode”-Standard. Sie wird auch als Phase 1.5 und Transaktionsvermittlung bezeichnet. Diese Funktion steht in Windows 95 nicht zur Verfügung.

Die PGPnet-Funktion “Virtuelle Identität” kann von einem sicheren Gateway aus IP-Adressen und weitere Konfigurationsinformationen für Ihren Computer abrufen. Da der Gateway Ihrem Computer eine Adresse zuweist, werden Sie von allen Computern hinter dem Gateway als Teil Ihres Netzwerks angesehen, und diese können ungehindert mit Ihnen kommunizieren.

Um eine Verbindung zu einem sicheren Gateway aufzubauen, bei dem die Funktion zum Abrufen der virtuellen Identität aktiviert ist, müssen Sie manuell auf **Verbinden** auf der Registerkarte **VPN** klicken.

Sie können die Einstellung für das Abrufen der virtuellen Identität eines Gateway-Hosteintrags jederzeit durch Klicken auf die Schaltfläche **Eigenschaften** auf der Registerkarte **VPN** ändern.

Wenn die Funktion “Virtuelle Identität” verwendet werden soll, klicken Sie auf **Abrufen der virtuellen Identität für diesen Gateway aktivieren**.

Wenn Sie die virtuelle Identität nicht abrufen lassen möchten, fahren Sie mit Schritt 12 fort.

11. **Neuen Gateway-Eintrag als exklusiven Gateway erstellen.** Diese Option wird nur angezeigt, wenn Sie einen Eintrag für einen Gateway hinzufügen. Bei der Verbindung zu einem exklusiven Gateway tunnelt PGPnet sämtlichen Verkehr (lokal und nicht lokal) zu diesem Gateway.

HINWEIS: Diese Funktion steht in Windows 95 nicht zur Verfügung.

Beachten Sie, daß Sie nach dem Hinzufügen eines exklusiven Gateways auf die Schaltfläche **Verbinden** auf der Registerkarte **VPN** klicken müssen, um die Verbindung zu diesem Gateway aufzubauen.

Wenn ein exklusiver Gateway wieder in einen nicht-exklusiven Gateway umgewandelt werden soll, müssen Sie den Hosteintrag auf der Registerkarte **VPN** ändern.

Wenn Sie möchten, daß der Eintrag ein exklusiver Gateway wird, müssen Sie auf **Neuen Gateway-Eintrag als exklusiven Gateway erstellen** klicken.

Der Assistent fragt, ob Sie einen Eintrag für einen Host oder ein Teilnetz hinter dem Gateway hinzufügen möchten. Wenn dies der Fall ist, wählen Sie **Ja**. Befolgen Sie dann die Anweisungen des Assistenten.

12. Legen Sie fest, wie der Verbindungsaufbau zu diesem Host erfolgen soll:

    - **Automatisch verbinden:** Wählen Sie diese Option, wenn PGPnet bei jeder Paketsendung an den Hosteintrag automatisch die Verbindung herstellen soll.
    - **Manuelle Verbindung anfordern:** Wählen Sie diese Option, wenn Sie Ihren Computer an mehreren Standorten einsetzen (z. B. als Firmenmitarbeiter, der seinen Laptop sowohl im Büro als auch zu Hause nutzt). Diese Funktion ermöglicht eine sichere Kommunikation mit denselben Hosts von beiden Seiten eines Firmen-Gateways unter Nutzung eines der beiden Adapter Ihres Computers. Zum manuellen Verbindungsaufbau verwenden Sie die Schaltfläche **Verbinden** auf der Registerkarte **VPN**.

13. Klicken Sie auf **OK**, um den Eintrag der Hostliste in PGPnet hinzuzufügen.

Host-, Teilnetz- oder Gateway-Eintrag ändern

Es kann passieren, daß Sie die Konfiguration eines Hosts, eines Teilnetzes oder eines Gateways bearbeiten müssen. Dies ist beispielsweise der Fall, wenn sich eine IP-Adresse, Teilnetz-Maske oder ein Host-Domänenname ändert. So bearbeiten Sie eine Konfiguration:

1. Klicken Sie auf die Registerkarte **VPN**.
2. Wählen Sie den Host-, Teilnetz- oder Gateway-Eintrag aus, den Sie bearbeiten möchten.
3. Klicken Sie auf **Eigenschaften**.

TIP: Statt einen Host auszuwählen und auf **Eigenschaften** zu klicken, können Sie auch auf den Hosteintrag in der Hostliste doppelklicken.

---

4. Nehmen Sie die gewünschten Änderungen vor.
5. Klicken Sie auf **OK**.

   Die PGPnet-Datenbank wird umgehend aktualisiert. Die PGPnet-Datenbank wird jedoch erst aktualisiert, wenn die ordnungsgemäße Funktionsweise des PGPnet-Services oder des -Treibers gewährleistet ist. Hierzu ist unter Umständen ein Neustart des Computers erforderlich.

Host-, Teilnetz- oder Gateway-Eintrag entfernen

Es kann vorkommen, daß Sie einen konfigurierten Host oder ein konfiguriertes Teilnetz bzw. einen Gateway entfernen müssen. Dies ist beispielsweise der Fall, wenn Sie bezüglich eines bestimmten Objekts Sicherheitsbedenken haben. So entfernen Sie einen Host, ein Teilnetz oder einen Gateway:

1. Klicken Sie auf die Registerkarte **VPN**.
2. Wählen Sie den Host-, Teilnetz- oder Gateway-Eintrag aus, den Sie entfernen möchten.
3. Klicken Sie auf **Entfernen**.

Expert-Modus: Hosts, Gateways oder Teilnetze ohne Assistenten hinzufügen

HINWEIS: In Unternehmensumgebungen kann der **Expert-Modus** des Assistenten vom PGP-Administrator deaktiviert worden sein.

Wenn Sie sich mit PGPnet vertraut gemacht haben, können Sie Hosts, Gateways und Teilnetze auch im **Expert-Modus** hinzufügen und bearbeiten und auf diese Weise Zeit sparen. Im Gegensatz zum Assistenten, der Ihnen Schritt für Schritt erklärt, wie Sie Einträge hinzufügen, wird im **Expert-Modus** nur ein Formular für den neuen Eintrag angezeigt.

HINWEIS: Bei der Verwendung des **Expert-Modus** müssen Sie einen Authentisierungsschlüssel oder ein Authentisierungszertifikat auswählen, sofern dies noch nicht geschehen ist (**Ansicht—>Optionen—> PGPnet-Authentisierung**).

- Wie Sie den Expert-Modus aktivieren bzw. deaktivieren können, erfahren Sie im Abschnitt siehe “Expert-Modus aktivieren und deaktivieren” auf Seite 235.
- Informationen zur Funktion “DNS-Suche” finden Sie im Abschnitt siehe “DNS-Suche: IP-Adresse eines Hosts suchen” auf Seite 236.
- Informationen zum gemeinsamen Geheimnis finden Sie im Abschnitt siehe “Gemeinsames Geheimnis” auf Seite 237.
- Informationen zur entfernten Authentisierung finden Sie im Abschnitt siehe “Entfernte Authentisierung” auf Seite 237.

Expert-Modus aktivieren und deaktivieren

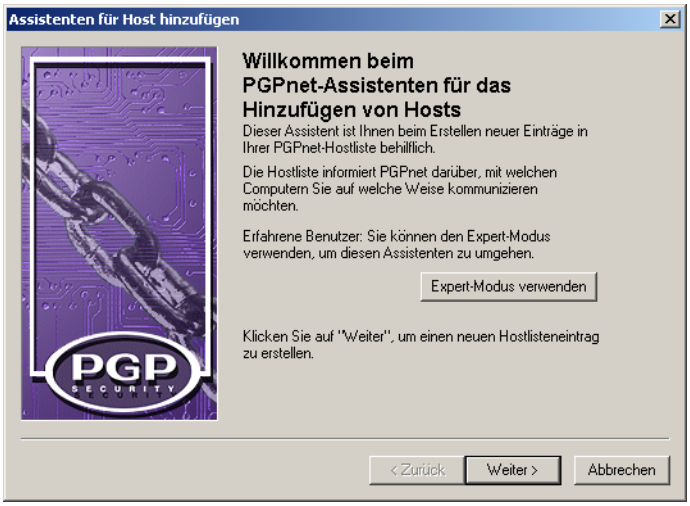


Abbildung 12-4. Assistent zum Hinzufügen von Hosts

So aktivieren Sie den Expert-Modus:

1. Klicken Sie auf die Registerkarte **VPN**.
2. Klicken Sie auf **Hinzufügen**.
3. Klicken Sie auf **Expert-Modus verwenden**. PGPnet zeigt das Dialogfeld “Host / Gateway” an.

So deaktivieren Sie den Expert-Modus:

1. Klicken Sie auf die Registerkarte **VPN**.
2. Klicken Sie auf **Hinzufügen**.
3. Klicken Sie auf **Assistent verwenden**. PGPnet zeigt den **Assistenten zum Hinzufügen von Hosts** an.

DNS-Suche: IP-Adresse eines Hosts suchen

Der Expert-Modus von PGPnet enthält eine DNS-Suchfunktion. Verwenden Sie diese Funktion, um nach der IP-Adresse eines Hosts zu suchen.

So verwenden Sie die DNS-Suchfunktion:

1. Klicken Sie auf der PGPnet-Registerkarte **VPN** auf **Hinzufügen**. Wenn der **Assistent zum Hinzufügen von Hosts** angezeigt wird, klicken Sie auf **Expert-Modus verwenden**.
2. Klicken Sie auf **DNS-Suche**. PGPnet zeigt das Dialogfeld “DNS-Suche” an.

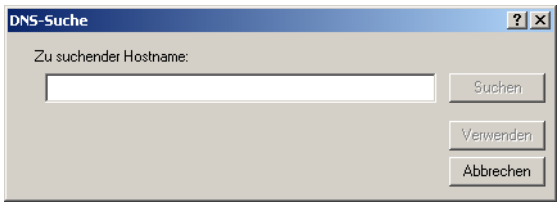


Abbildung 12-5. Dialogfeld “DNS-Suche”

3. Geben Sie den Hostnamen des Systems in das Feld **Zu suchender Hostname** ein, und klicken Sie anschließend auf **Suchen**. PGPnet sucht die IP-Adresse des von Ihnen eingegebenen Hostnamens.
   - Wird diese gefunden, zeigt PGPnet sie gleich an. Klicken Sie auf **Verwenden**, um die IP-Adresse im Dialogfeld “Host / Gateway” zu verwenden.
   - Wenn keine IP-Adresse gefunden wird, erhalten Sie eine entsprechende Meldung.

> **TIP:** Sie können den Hostnamen des Systems in das Namensfeld im Dialogfeld “Host / Gateway” eingeben und anschließend auf **DNS-Suche** klicken. Daraufhin wird das Fenster **DNS-Suche** angezeigt. Klicken Sie auf **Suchen**, um die IP-Adresse des von Ihnen eingegebenen Hostnamens zu suchen.

Gemeinsames Geheimnis

WARNUNG: Im Gegensatz zu herkömmlichen PGP-Paßphrasen werden gemeinsame geheime Paßphrasen unverschlüsselt auf dem Computer gespeichert. Dies stellt ein mögliches Sicherheitsrisiko dar. Verwenden Sie Schlüssel oder Zertifikate, um diesem Risiko vorzubeugen.

Für eine mit einer gemeinsamen geheimen Paßphrase gesicherte Kommunikation müssen beide Benutzer in der Hostliste von PGPnet einen Eintrag für das jeweils andere System erstellen. Hierzu muß Ihnen der Hostname oder die IP-Adresse des anderen Systems bekannt sein, und Sie müssen sich auf eine gemeinsame geheime Paßphrase verständigen.

Entfernte Authentisierung

Vorlage eines bestimmten Schlüssels oder eines bestimmten Zertifikats vom Host fordern

Mit den Optionen im Abschnitt **Entfernte Authentisierung** des Dialogfelds “Host / Gateway” können Sie festlegen, daß der entfernte Host jedesmal einen bestimmten PGP-Schlüssel oder ein bestimmtes X.509-Zertifikat angeben muß, wenn er die Einrichtung einer SA mit Ihrem Host versucht. Wenn der Host dann versucht, eine Verbindung aufzubauen und dabei nicht den festgelegten Schlüssel bzw. das festgelegte Zertifikat vorlegt, verweigert Ihr Rechner den Verbindungsaufbau. Die Standardeinstellung ist **Beliebiger gültiger Schlüssel**.

Sie können diese Einstellung bereits beim Hinzufügen des Hosts im Expert-Modus oder aber später durch Bearbeiten des entsprechenden Hosteintrags vornehmen.

HINWEIS: Denken Sie daran, daß der Host seinen eigenen öffentlichen Schlüssel, nicht Ihren, vorlegen muß.

So legen Sie fest, daß ein Host einen bestimmten Schlüssel oder ein bestimmtes Zertifikat vorlegen muß:

1. Falls nicht bereits geschehen, fügen Sie PGPnet den Host, das Teilnetz oder den Gateway hinzu (Anweisungen dazu finden Sie in siehe “Host hinzufügen” auf Seite 227 und “Teilnetz oder Gateway hinzufügen” auf Seite 229). PGPnet fügt der Hostliste auf der Registerkarte **VPN** einen Eintrag hinzu.

2. Wählen Sie den Eintrag auf der Registerkarte **VPN** aus, und klicken Sie auf **Eigenschaften**. PGPnet zeigt das Dialogfeld “Host/Gateway” an. Der Abschnitt **Entfernte Authentisierung** befindet sich im Dialogfeld unten.

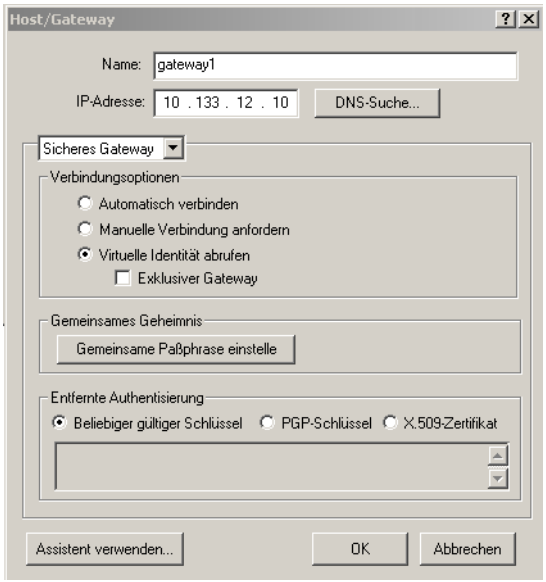


Abbildung 12-6. Dialogfeld “Host/Gateway”

3. Sie können für die eigene Authentisierung vom Host, Teilnetz oder Gateway einen bestimmten PGP-Schlüssel oder ein bestimmtes X.509-Zertifikat verlangen.

   - Um einen bestimmten PGP-Schlüssel anzufordern, klicken Sie auf **PGP-Schlüssel**. PGPnet zeigt das Dialogfeld “Schlüssel auswählen” an. Wählen Sie den entsprechenden Schlüssel aus, und klicken Sie anschließend auf **OK**. PGPnet zeigt den Schlüssel im Feld **Entfernte Authentisierung** an. Klicken Sie auf **OK**, um das Dialogfeld “Host/Gateway” zu schließen.

   - Um ein bestimmtes X.509-Zertifikat zu fordern, klicken Sie auf **X.509-Zertifikat**. PGPnet zeigt das Dialogfeld **X.509-Zertifikat auswählen** an. Klicken Sie auf das entsprechende Zertifikat, und klicken Sie anschließend auf **OK**. PGPnet zeigt das Zertifikat im Feld **Entfernte Authentisierung** an. Klicken Sie auf **OK**, um das Dialogfeld “Host/Gateway” zu schließen.

WICHTIG: Wenn Sie für einen sicheren Teilnetzeintrag einen bestimmten PGP-Schlüssel oder ein bestimmtes X.509-Zertifikat wählen, müssen alle Benutzer in diesem Teilnetz den gleichen Schlüssel benutzen, um sich zu authentisieren.

Alle Schlüsselauthentisierungen werden auf der Registerkarte **Protokoll** angezeigt, und für jeden Eintrag wird die Schlüssel-ID angezeigt.

Die Funktionen “Abrufen der virtuellen Identität” und “Exklusiver Gateway”

HINWEIS: Die PGPnet-Funktion “Virtuelle Identität” basiert auf dem von der IPsec-Arbeitsgruppe der IETF entworfenen “config-mode”-Standard. Sie wird auch als Transaktionsvermittlung bezeichnet.

Wenn Sie von zu Hause aus oder in einem Büro arbeiten, das nicht direkt in das Unternehmensnetzwerk eingebunden ist, können Sie mit Hilfe der Funktion **Abrufen der virtuellen Identität** auf Ihr Unternehmensnetzwerk zugreifen. Wenn diese Funktion aktiv ist, nimmt PGPnet Kontakt mit dem Gateway auf und ruft eine IP-Adresse und die Namen der DNS- und WINS-Server für Ihren Computer ab. Da die Adresse und die Servernamen Ihrem Computer vom Gateway zugewiesen werden, werden Sie von allen Computern hinter dem Gateway als Teil Ihres Netzwerks angesehen, und diese können ungehindert mit Ihnen kommunizieren. Die Verbindung zu Ihrem Unternehmens-
Gateway erfolgt via Tunnelmodus.

Bei der Verbindung zu einem **exklusiven Gateway** tunnelt PGPnet sämtlichen lokalen und nicht-lokalen Verkehr zu diesem Gateway. Für Sie gelten die gleichen Sicherungsmaßnahmen und Einschränkungen durch die Unternehmens-Firewall, wie für die Benutzer in der “Zentrale”.

Beachten Sie, daß Sie nach dem Hinzufügen eines exklusiven Gateways auf die Schaltfläche **Verbinden** auf der **Registerkarte VPN** klicken müssen, um die Verbindung zu diesem Gateway aufzubauen. Wenn Sie eine Verbindung zu einem exklusiven Gateway herstellen, bleiben zwar alle vorhandenen SAs für Hosts, die sich nicht im lokalen Teilnetz befinden, bestehen, sie werden dabei aber ungültig.

Teil V: Anhänge und Glossar

- **Anhang A: Optionen festlegen**
- **Anhang B: Problembehebung in PGP**
- **Anhang C: Problembehebung in PGPnet**
- **Anhang D: Von der PGPnet-Funktion IDS erkannte häufig vorkommende Angriffe**
- **Anhang E: Liste biometrischer Worte**
- **Glossar**

Optionen festlegen A

In diesem Kapitel wird beschrieben, wie Sie die PGP-Optionen den Anforderungen Ihrer persönlichen Computerumgebung anpassen können.

Optionen:	**Siehe:**
Allgemeine Optionen	“Allgemeine Optionen festlegen” auf Seite 244
Dateioptionen	“Dateioptionen festlegen” auf Seite 248
E-Mail-Optionen	“E-Mail-Optionen festlegen” auf Seite 250
HotKey-Optionen	“HotKey-Optionen festlegen” auf Seite 253
Serveroptionen	“Serveroptionen festlegen” auf Seite 255
CA-Optionen	“CA-Optionen festlegen” auf Seite 258
Erweiterte Optionen	“Erweiterte Optionen festlegen” auf Seite 259
Optionen für die persönliche Firewall	“Optionen für die persönliche Firewall festlegen” auf Seite 263
Optionen für das persönliche IDS	“Optionen für das persönliche IDS festlegen” auf Seite 263
VPN-Optionen	“VPN-Optionen festlegen” auf Seite 263
Optionen für die VPN-Authentisierung	“Optionen für die VPN-Authentisierung festlegen” auf Seite 267
Erweiterte VPN-Optionen	“Optionen auf der Registerkarte “VPN – Erweitert” festlegen” auf Seite 270
PGPdisk-Optionen	“PGPdisk-Optionen festlegen” auf Seite 279

PGP-Optionen festlegen

Obwohl PGP bereits auf die Bedürfnisse der meisten Benutzer ausgelegt ist, haben Sie die Möglichkeit, einige Einstellungen den Anforderungen Ihrer persönlichen Computerumgebung anzupassen. Das Anpassen dieser Einstellungen erfolgt im Dialogfeld “PGP-Optionen”.

Das Dialogfeld “PGP-Optionen” kann auf verschiedene Art und Weise geöffnet werden:

- Wenn Sie in einem der PGP-Dienstprogramme oder einem Programm mit einem PGP-Plugin arbeiten, klicken Sie in PGPtray auf das graue Schloßsymbol ( ), und wählen Sie den Befehl **Optionen**.
- Wenn Sie in PGPkeys arbeiten, wählen Sie den Befehl **Optionen** aus dem Menü **Bearbeiten**.
- Wenn Sie in PGPnet arbeiten, wählen Sie den Befehl **Optionen** aus dem Menü **Ansicht**.
- Wenn Sie im PGPdisk-Editor arbeiten, wählen Sie den Befehl **Optionen** aus dem Menü **Datei**.

Allgemeine Optionen festlegen

Auf der Registerkarte **Allgemein** können Sie Einstellungen für das Verschlüsseln, Unterschreiben, Anmelden und endgültige Löschen von Dateien festlegen.

So legen Sie die allgemeinen PGP-Optionen fest:

1. Öffnen Sie das Dialogfeld “PGP-Optionen”.

Wenn das Dialogfeld “PGP-Optionen” geöffnet wird, wird zunächst die Registerkarte **Allgemein** angezeigt (siehe Abbildung A-1).

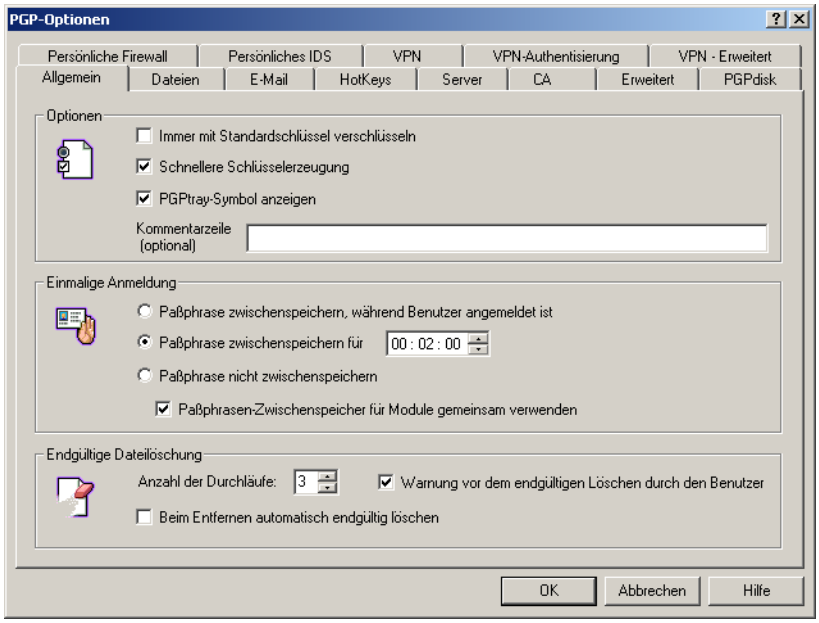


Abbildung A-1. Dialogfeld “PGP-Optionen” (Registerkarte “Allgemein”)

2. Auf dieser Registerkarte können die folgenden PGP-Optionen festgelegt werden:

Verschlüsselungsoptionen

- **Immer mit Standardschlüssel verschlüsseln:** Wenn diese Option aktiviert ist, werden alle E-Mail-Nachrichten und Dateianhänge, die Sie mit einem öffentlichen Schlüssel eines Empfängers verschlüsseln, auch für Sie mit Ihrem öffentlichen Standardschlüssel verschlüsselt. Sie sollten diese Option aktiviert lassen, damit Sie den Inhalt jeder beliebigen E-Mail-Nachricht oder Datei, die Sie zuvor verschlüsselt haben, entschlüsseln können.

- **Schnellere Schlüsselerzeugung:** Wenn diese Option aktiviert ist, wird weniger Zeit zum Erzeugen eines neuen Diffie-Hellman / DSS-Schlüsselpaares benötigt. Dieser Prozeß wird beschleunigt, indem die Schlüssel mit Hilfe eines zuvor berechneten Primzahlsatzes erstellt werden und die zeitaufwendige Primzahlberechnung bei der Schlüsselerstellung somit übersprungen wird. Dabei ist aber zu beachten, daß die schnellere Schlüsselerzeugung nur für Schlüsselgrößen über 1024 und unter 4096 implementiert ist. Obwohl es für andere Personen nahezu unmöglich ist, Ihren Schlüssel mit Hilfe des zuvor berechneten Primzahlsatzes zu dekodieren, sollten Sie zusätzlich ein Schlüsselpaar mit maximalen Sicherheitsvorkehrungen erstellen.

  In der Verschlüsselungstechnik wird im allgemeinen davon ausgegangen, daß die Verwendung solcher vorgefertigter Primzahlsätze für Diffie-Hellman / DSS-Algorithmen keinen Verlust an Sicherheit mit sich bringt. Wenn Sie mit dieser Funktion nicht arbeiten möchten, deaktivieren Sie sie.

- **PGPtray-Symbol anzeigen:** Wenn diese Option aktiviert ist, können Sie viele der PGP-Funktionen über das PGPtray-Symbol in der Task-Leiste aufrufen.

- **Kommentarzeile:** In diesem Bereich können Sie Kommentare hinzufügen. Der hier eingegebene Text wird dann immer in Nachrichten und Dateien eingefügt, die Sie verschlüsseln oder unterschreiben. Der Text wird unter dem Kopf BEGIN PGP MESSAGE BLOCK und der PGP-Versionsnummer jeder Nachricht angezeigt.

Einmalige Anmeldung

- **Paßphrase zwischenspeichern, während Benutzer angemeldet ist:** Speichert Ihre Paßphrase automatisch so lange im Arbeitsspeicher, bis Sie Ihren Computer wieder abmelden. Wenn Sie diese Option wählen, werden Sie für jede erste Unterschrifts- und Entschlüsselungsaufgabe einmal nach Ihrer Paßphrase gefragt. Bis Sie Ihren Computer wieder abmelden, müssen Sie dann für ein und dieselbe Aufgabe Ihr Paßwort nicht wieder eingeben.

WICHTIG: Wenn diese Option aktiviert ist, müssen Sie unbedingt darauf achten, Ihren Computer abzumelden, wenn Sie ihn unbeaufsichtigt lassen. Wenn Sie sich nie abmelden, verbleibt Ihre Paßphrase wochenlang im Zwischenspeicher. Sind Sie dann nicht an Ihrem Computer, kann jeder Ihre verschlüsselten Nachrichten lesen bzw. Nachrichten mit Ihrem Schlüssel verschlüsseln.

- **Paßphrase zwischenspeichern für:** Speichert Ihre Paßphrase automatisch für die angegebene Zeitspanne (in Stunden: Minuten: Sekunden) im Arbeitsspeicher. Wenn Sie diese Option wählen, werden Sie für die erste Unterschrifts- bzw. Entschlüsselungsaufgabe einmal nach Ihrer Paßphrase gefragt. Danach müssen Sie Ihre Paßphrase erst wieder eingeben, wenn die von Ihnen festgelegte Zeitspanne abgelaufen ist. Der Standardwert beträgt 2 Minuten.
- **Paßphrase nicht zwischenspeichern:** Wenn Sie diese Option aktivieren, wird Ihre Paßphrase überhaupt nicht im Arbeitsspeicher gespeichert. Sie müssen dann für sämtliche PGPnet-Kommunikation sowie für alle Verschlüsselungs-, Unterzeichnungs- und Entschlüsselungsaufgaben Ihre Paßphrase neu eingeben.
- **Paßphrasen-Zwischenspeicher für Module gemeinsam verwenden:** Speichert Ihre Paßphrase automatisch im Arbeitsspeicher und läßt die Nutzung von den verschiedenen PGP-Modulen zu. Wenn Sie Ihre Paßphrase beispielsweise zum Unterschreiben in PGPtools verwenden, müssen Sie sie zum Entschlüsseln in PGPtray nicht erneut eingeben. Wenn Sie diese Option zusammen mit der Option **Paßphrase zwischenspeichern, während Benutzer angemeldet ist** aktivieren, wird Ihre Paßphrase so lange im Arbeitsspeicher gespeichert, bis Sie Ihren Computer abmelden. Sie können diese Option aber auch zusammen mit der Option **Paßphrase zwischenspeichern für** aktivieren und dann eine Zeitdauer festlegen, für die Ihre Paßphrase gespeichert werden soll.

Endgültige Dateilöschung

- **Anzahl der Durchläufe:** Mit dieser Einstellung wird gesteuert, wie oft die Programme zum endgültigen Löschen über die Festplatte laufen sollen.
- **Warnung vor dem endgültigen Löschen durch den Benutzer:** Wenn diese Einstellung aktiviert ist, wird vor dem unwiederherstellbaren Löschen einer Datei ein Dialogfeld angezeigt, um Ihnen noch eine letzte Möglichkeit zu geben, den Vorgang abzubrechen, bevor PGP den Inhalt der Datei überschreibt und sie von Ihrer Festplatte löscht.
- **Beim Entfernen automatisch endgültig löschen:** Wenn Sie eine Datei wie üblich durch Verschieben in den Papierkorb löschen, wird nur der Name der Datei aus dem Dateiverzeichnis entfernt, der Inhalt der Datei verbleibt jedoch auf der Festplatte. Wenn Sie die Option **Beim Entfernen automatisch endgültig löschen** aktivieren, wird der Inhalt des Papierkorbs beim Leeren endgültig gelöscht, so daß die gelöschten Elemente nicht wiederhergestellt werden können.

- **Status anzeigen:** Zeigt beim endgültigen Löschen von Dateien aus dem Papierkorb einen Verlaufsbalken an. Diese Option ist nur dann verfügbar, wenn die Option **Beim Entfernen automatisch endgültig löschen** aktiviert ist.

3. Klicken Sie auf **OK**, um Ihre Änderungen zu speichern und zum Hauptfenster von PGPkeys zurückzukehren, oder wählen Sie eine andere Registerkarte, um mit dem Konfigurieren Ihrer PGP-Optionen fortzufahren.

Dateioptionen festlegen

Verwenden Sie die Registerkarte **Dateien**, um den Pfad der Schlüsselbunddateien anzugeben, in denen Ihre privaten und öffentlichen Schlüssel gespeichert sind.

So legen Sie die PGP-Dateioptionen fest:

1. Öffnen Sie das Dialogfeld “PGP-Optionen”, und klicken Sie auf die Registerkarte **Dateien**.

   Das Dialogfeld “Optionen” wird mit geöffneter Registerkarte **Dateien** angezeigt (siehe Abbildung A-2).

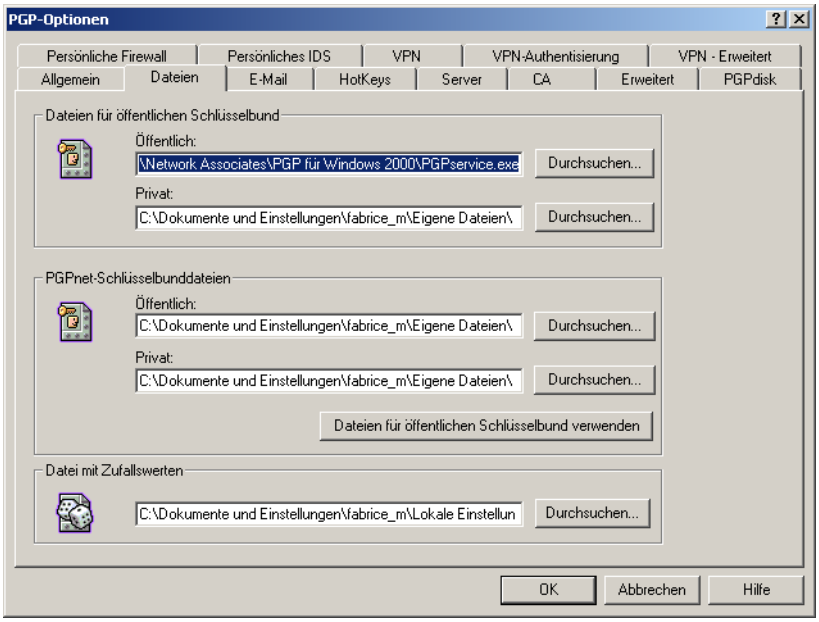


Abbildung A-2. Dialogfeld “PGP-Optionen” (Registerkarte “Dateien”)

2. Mit den Schaltflächen auf der Registerkarte **Dateien** können Sie die Pfade zu Ihren öffentlichen und privaten Schlüsselbunden bzw. zur Datei mit den Zufallswerten angeben:

Dateien für öffentlichen Schlüsselbund

- **Öffentliche Schlüsselbunddatei:** In diesem Feld werden der Name der Datei und der Speicherort angezeigt, an dem PGP Ihre öffentliche Schlüsselbunddatei erwartet. Wenn Sie Ihre öffentlichen Schlüssel in einer Datei mit einem anderen Namen oder an einem anderen Ort speichern möchten, geben Sie diese Informationen hier an. In dem von Ihnen angegebenen Verzeichnis werden auch alle automatisch erstellten Sicherheitskopien des öffentlichen Schlüsselbundes gespeichert. Weitere Informationen zum automatischen Sichern Ihrer Schlüsselbunde finden Sie im Abschnitt “Erweiterte Optionen festlegen” auf Seite 259.

- **Private Schlüsselbunddatei:** In diesem Feld werden der Name der Datei und der Speicherort angezeigt, an dem PGP Ihre private Schlüsselbunddatei erwartet. Wenn Sie Ihre privaten Schlüssel in einer Datei mit einem anderen Namen oder an einem anderen Ort speichern möchten, geben Sie diese Informationen hier an. Einige Benutzer bewahren ihren privaten Schlüsselbund auf einer Diskette auf, die sie wie einen Schlüssel einlegen, wenn sie eine E-Mail-Nachricht unterzeichnen oder entschlüsseln müssen. In dem von Ihnen angegebenen Verzeichnis werden auch alle automatisch erstellten Sicherheitskopien des öffentlichen Schlüsselbundes gespeichert.

PGPnet-Schlüsselbunddateien

- **Öffentliche Schlüsselbunddatei**: In diesem Feld werden der Name der Datei und der Speicherort angezeigt, an dem PGPnet Ihre öffentliche Schlüsselbunddatei erwartet. Wenn Sie Ihre öffentlichen Schlüssel in einer Datei mit einem anderen Namen oder an einem anderen Ort speichern möchten, geben Sie diese Informationen hier an. In dem von Ihnen angegebenen Verzeichnis werden auch alle automatisch erstellten Sicherheitskopien des öffentlichen Schlüsselbundes gespeichert. Weitere Informationen zum automatischen Sichern Ihrer Schlüsselbunde finden Sie im Abschnitt “Erweiterte Optionen festlegen” auf Seite 259.

- **Private Schlüsselbunddatei:** In diesem Feld werden der Name der Datei und der Speicherort angezeigt, an dem PGPnet Ihre private Schlüsselbunddatei erwartet. Wenn Sie Ihre privaten Schlüssel in einer Datei mit einem anderen Namen oder an einem anderen Ort speichern möchten, geben Sie diese Informationen hier an. Einige Benutzer bewahren ihren privaten Schlüsselbund auf einer Diskette auf, die sie wie einen Schlüssel einlegen, wenn sie eine E-Mail-Nachricht unterzeichnen oder entschlüsseln müssen. In dem von Ihnen angegebenen Verzeichnis werden auch alle automatisch erstellten Sicherheitskopien des öffentlichen Schlüsselbundes gespeichert.

  Über die Schaltfläche **Dateien für öffentlichen Schlüsselbund verwenden** können Sie Ihre PGPnet-Schlüsselbunde automatisch auf dieselben Schlüsselbunddateien einstellen, die für das übrige PGP-Programm verwendet werden.

Datei mit Zufallswerten

- **Datei mit Zufallswerten:** Gibt den Speicherort der Datei mit Zufallswerten an. Aus Sicherheitsgründen speichern einige Benutzer ihre Datei mit Zufallswerten in einem sicheren Pfad. Da ein unbefugter Zugriff auf diese Datei sehr schwierig ist und PGP dagegen schon Vorkehrungen getroffen hat, hat das Verschieben der Datei aus dem Standardverzeichnis nur begrenzten Wert.

3. Klicken Sie auf **OK**, um Ihre Änderungen zu speichern, oder wählen Sie eine andere Registerkarte, um mit dem Konfigurieren Ihrer PGP-Optionen fortzufahren.

E-Mail-Optionen festlegen

Auf der Registerkarte **E-Mail** können Sie die Optionen festlegen, mit denen die Art der Implementierung der PGP-Funktionen für Ihr spezielles E-Mail-Programm bestimmt wird. Unter Umständen lassen sich nicht alle der hier vorgenommenen Einstellungen in Ihrem E-Mail-Programm umsetzen.

So legen Sie E-Mail-Optionen fest:

1. Öffnen Sie das Dialogfeld “PGP-Optionen”, und klicken Sie auf die Registerkarte **E-Mail**.

   Das Dialogfeld “PGP-Optionen” wird mit geöffneter Registerkarte **E-Mail** angezeigt (siehe Abbildung A-3).

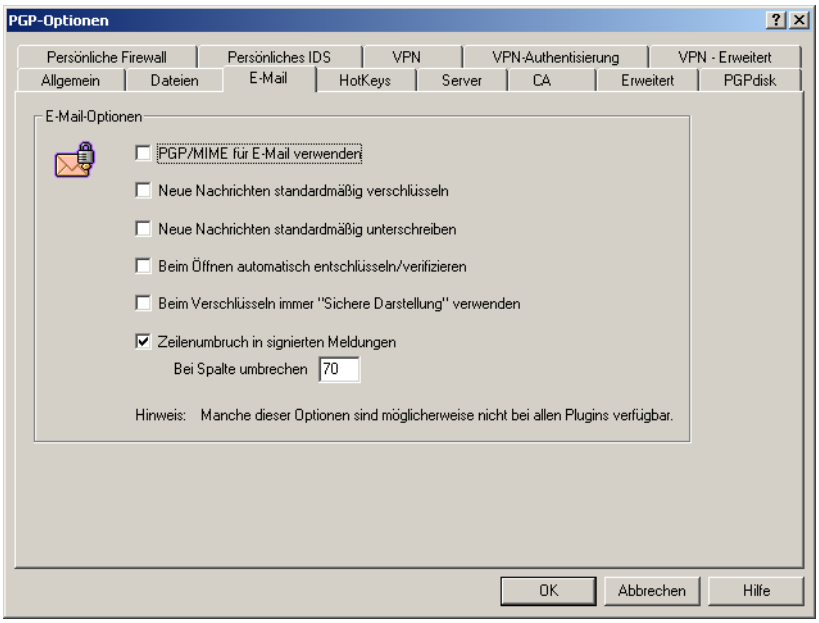


Abbildung A-3. Dialogfeld “PGP-Optionen” (Registerkarte “E-Mail”)

2. Legen Sie auf der Registerkarte **E-Mail** die gewünschten Verschlüsselungsoptionen fest. Folgende Optionen stehen zur Verfügung:

   - **PGP/MIME für E-Mail verwenden:** Wenn Sie Eudora verwenden und diese Einstellung aktivieren, werden alle E-Mail-Nachrichten und Dateianhänge automatisch für den gewünschten Empfänger verschlüsselt. Diese Einstellung wirkt sich nicht auf andere Verschlüsselungen aus, die Sie über die Zwischenablage oder mit dem Windows-Explorer durchführen. Sie sollte nicht verwendet werden, wenn Sie E-Mail-Nachrichten an Empfänger senden möchten, deren E-Mail-Programme den PGP / MIME-Standard nicht unterstützen. In Eudora werden Dateianhänge unabhängig von dieser Einstellung stets verschlüsselt. Wenn der Empfänger jedoch nicht über PGP / MIME verfügt, muß die Entschlüsselung manuell erfolgen.

- **Neue Nachrichten standardmäßig verschlüsseln:** Wenn Sie diese Einstellung aktivieren, werden alle E-Mail-Nachrichten und Dateianhänge automatisch verschlüsselt. Von einigen E-Mail-Programmen wird diese Funktion nicht unterstützt.
- **Neue Nachrichten standardmäßig unterschreiben:** Wenn Sie diese Option aktivieren, werden Sie aufgefordert, alle Ihre E-Mail-Nachrichten zu unterschreiben. Von einigen E-Mail-Programmen wird diese Funktion nicht unterstützt. Diese Einstellung hat keine Auswirkung auf andere Unterschriften, die Sie mit Hilfe der Zwischenablage oder des Windows-Explorers hinzufügen.
- **Beim Öffnen automatisch entschlüsseln/verifizieren:** Wenn Sie diese Option aktivieren, werden alle verschlüsselten oder/und unterschriebenen E-Mail-Nachrichten und Dateianhänge automatisch entschlüsselt und verifiziert. Von einigen E-Mail-Programmen wird diese Funktion nicht unterstützt.
- **Beim Verschlüsseln immer "Sichere Darstellung" verwenden:** Wenn Sie diese Option wählen, werden alle Ihre entschlüsselten E-Mail-Nachrichten zur Verhinderung von TEMPEST-Attacken im Fenster "Sichere Darstellung" angezeigt und können nicht im entschlüsselten Format gespeichert werden. Weitere Informationen zu TEMPEST-Attacken finden Sie im Abschnitt zu Sicherheitsrisiken in der *Einführung in die Kryptographie*.
- **Zeilenumbruch in signierten Meldungen Bei Spalte umbrechen [ ]:** Mit dieser Einstellung wird die Spaltennummer festgelegt, an der der Text in der digitalen Unterschrift durch eine Absatzmarke umgebrochen wird. Diese Funktion ist erforderlich, da Zeilenumbrüche nicht bei allen Anwendungen auf die gleiche Weise vorgenommen werden, wodurch die Zeilen in Ihren digital unterschriebenen Nachrichten eventuell so umgebrochen werden, daß sie schwer lesbar sind. Bei der Standardeinstellung von 70 wird dieses Problem bei den meisten Anwendungen vermieden.

WARNUNG: Wenn Sie die Zeilenumbruch-Einstellung in PGP ändern, müssen Sie einen Wert wählen, der unter dem in Ihrem E-Mail-Programm eingestellten Wert liegt. Wenn der Wert gleich dem oder größer als der Wert Ihres E-Mail-Programms ist, werden möglicherweise Zeilenumbrüche eingefügt, die Ihre PGP-Unterschrift ungültig machen.

---

3. Klicken Sie auf **OK**, um Ihre Änderungen zu speichern, oder wählen Sie eine andere Registerkarte, um mit dem Konfigurieren Ihrer PGP-Optionen fortzufahren.

HotKey-Optionen festlegen

Verwenden Sie die Registerkarte **HotKeys**, um Tastaturbefehle für PGP-Funktionen festzulegen.

So legen Sie HotKey-Optionen fest:

1. Öffnen Sie das Dialogfeld “PGP-Optionen”, und klicken Sie auf die Registerkarte **HotKeys**.

   Das Dialogfeld “PGP-Optionen” wird mit geöffneter Registerkarte **HotKeys** angezeigt (siehe Abbildung A-4 auf Seite 253).

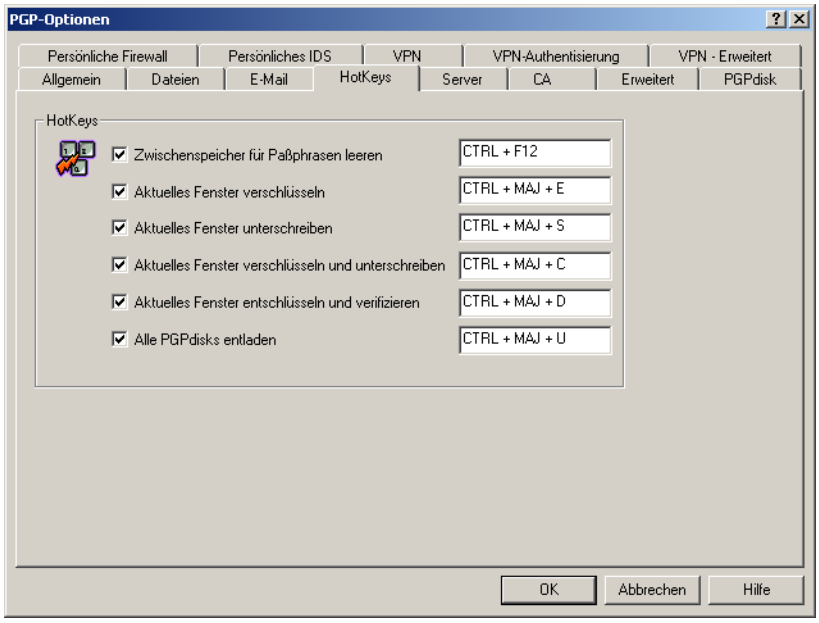


Abbildung A-4. Dialogfeld “PGP-Optionen” (Registerkarte “HotKeys”)

2. Wählen Sie die gewünschten HotKey-Optionen aus. Folgende Optionen stehen zur Verfügung:

   - **Zwischenspeicher für Paßphrasen leeren:** Wählen Sie diese Option, um einen HotKey zu erstellen, mit dem Sie den Cache-Speicher, der Ihre PGP-Entschlüsselungspaßphrase enthält, durch Betätigung einer oder mehrerer Tasten löschen können. Der Standard-HotKey für diese Funktion lautet STRG+F12.

   - **Aktuelles Fenster verschlüsseln:** Wählen Sie diese Option, um einen HotKey zu erstellen, mit dem Sie alle im aktuellen Fenster enthaltenen Daten durch Betätigung einer oder mehrerer Tasten verschlüsseln können. Der Standard-Hotkey für diese Funktion lautet STRG+UMSCHALT+E.

   - **Aktuelles Fenster unterschreiben:** Wählen Sie diese Option, um einen HotKey zu erstellen, mit dem Sie alle im aktuellen Fenster enthaltenen Daten durch Betätigung einer oder mehrerer Tasten unterschreiben können. Der Standard-HotKey für diese Funktion lautet STRG+UMSCHALT+S.

   - **Aktuelles Fenster verschlüsseln und unterschreiben:** Wählen Sie diese Option, um einen HotKey zu erstellen, mit dem Sie die im aktuellen Fenster enthaltenen Daten durch Betätigung einer oder mehrerer Tasten verschlüsseln und unterschreiben können. Der Standard-HotKey für diese Funktion lautet STRG+UMSCHALT+C.

   - **Aktuelles Fenster entschlüsseln und verifizieren:** Wählen Sie diese Option, um einen HotKey zu erstellen, mit dem Sie die im aktuellen Fenster enthaltenen geschützten Daten durch Betätigung einer oder mehrerer Tasten entschlüsseln und verifizieren können. Der Standard-HotKey für diese Funktion lautet STRG+UMSCHALT+D.

   - **Alle PGPdisks entladen** (verfügbar, wenn PGPdisk installiert ist)**:** Wählen Sie diese Option, um einen HotKey zu erstellen, mit dem Sie durch Betätigung einer oder mehrerer Tasten alle Ihre PGPdisks auf einmal entladen können. Der Standard-HotKey für diese Funktion lautet STRG+UMSCHALT+U.

3. Klicken Sie auf **OK**, um Ihre Änderungen zu speichern, oder wählen Sie eine andere Registerkarte, um mit dem Konfigurieren Ihrer PGP-Optionen **fortzufahren**.

Serveroptionen festlegen

Auf der Registerkarte **Server** können Sie Einstellungen für die öffentlichen Schlüsselserver festlegen, die Sie zum Senden und Abrufen öffentlicher Schlüssel und zum automatischen Synchronisieren von Schlüsseln verwenden.

So legen Sie Schlüsselserver-Optionen fest:

1. Öffnen Sie das Dialogfeld “PGP-Optionen”, und klicken Sie auf die Registerkarte **Server**.

   Das Dialogfeld “PGP-Optionen” wird mit geöffneter Registerkarte **Server** angezeigt (siehe Abbildung A-5).

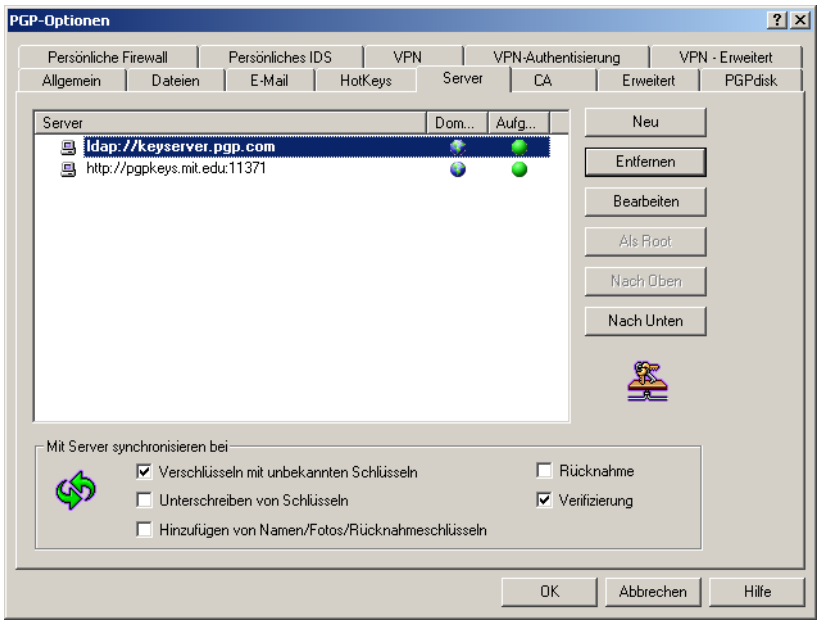


Abbildung A-5. Dialogfeld “PGP-Optionen” (Registerkarte “Server”)

2. Verwenden Sie zum Festlegen der Serveroptionen die folgenden Schaltflächen:

   - **Neu:** Fügt Ihrer Liste einen neuen Server hinzu.
   - **Entfernen:** Entfernt den gegenwärtig gewählten Server aus der Liste.
   - **Bearbeiten:** Ermöglicht das Bearbeiten der Serverinformationen für den ausgewählten Server.
   - **Als Root:** Gibt den Root-Server an, der für bestimmte firmeninterne Operationen (z. B. Aktualisieren und Senden von Gruppenlisten, Aktualisieren von Schlüsselverwaltern usw.) benötigt wird. In einer Firmenumgebung ist diese Option bereits von Ihrem Sicherheitsbeauftragten konfiguriert worden.
   - **Nach Oben** und **Nach Unten**: Verwenden Sie diese Schaltflächen, um die Server nach Belieben anzuordnen.

3. Legen Sie die Optionen fest, die für das Synchronisieren Ihres privaten Schlüsselbundes mit Ihren Schlüsselservern gelten sollen. Folgende Optionen stehen zur Verfügung:

Mit Server synchronisieren bei

- **Verschlüsseln mit unbekannten Schlüsseln:** Wenn Sie diese Option wählen, sucht PGP automatisch auf dem Server nach unbekannten Empfängern, um Benutzer zu finden, die sich nicht an Ihrem Schlüsselbund befinden, wenn eine E-Mail-Nachricht verschlüsselt wird.
- **Unterschreiben von Schlüsseln:** Wenn Sie diese Option wählen, werden Schlüssel, denen Sie Ihre Unterschrift hinzufügen, zuerst vom Server aktualisiert. Nach Beendigung der Aktualisierung werden die von Ihnen vorgenommenen Änderungen an den Server gesendet.
- **Hinzufügen von Namen/Fotos/Rücknahmeschlüsseln:** Wenn Sie diese Option wählen, werden Schlüssel, denen Sie Namen, Fotos oder Rücknahmeschlüssel hinzugefügt haben, zuerst vom Server aktualisiert. Nach Beendigung der Aktualisierung werden die von Ihnen vorgenommenen Änderungen an den Server gesendet. Durch die vorherige Aktualisierung wird sichergestellt, daß der Schlüssel seit der letzten Aktualisierung nicht zurückgenommen wurde.
- **Rücknahme:** Wenn Sie diese Option wählen, werden zurückgenommene Schlüssel zuerst vom Server aktualisiert. Nach Beendigung der Aktualisierung werden die von Ihnen vorgenommenen Änderungen an den Server gesendet.

- **Verifizierung:** Wenn Sie diese Option wählen, sucht und importiert PGP automatisch vom Schlüsselserver, wenn eine unterschriebene E-Mail-Nachricht oder -Datei verifiziert wird, für die Sie nicht den öffentlichen Schlüssel des Absenders besitzen.

4. Klicken Sie auf **OK**, um Ihre Änderungen zu speichern, oder wählen Sie eine andere Registerkarte, um mit dem Konfigurieren Ihrer PGP-Optionen fortzufahren.

So fügen Sie der Serverliste einen Schlüsselserver hinzu:

1. Öffnen Sie das Dialogfeld “PGP-Optionen”, und klicken Sie auf die Registerkarte **Server**.
2. Klicken Sie auf die Schaltfläche **Neu**.

   Das Dialogfeld “Neuen Server hinzufügen” wird angezeigt.
3. Wählen Sie im Feld **Typ** den Servertyp aus, der zum Zugriff auf den Server verwendet werden soll.

   - **PGP-Schlüsselserver-HTTP:** Wählen Sie diese Option, wenn Sie zum Speichern und Abrufen von PGP-Schlüsseln einen web-basierten PGP-Schlüsselserver verwenden.
   - **PGP-Schlüsselserver-LDAP:** Wählen Sie diese Option, wenn Sie zum Speichern und Abrufen von PGP-Schlüsseln einen PGP-Schlüsselserver über LDAP verwenden.
   - **PGP-Schlüsselserver-LDAPS:** Wählen Sie diese Option, wenn Sie zum Speichern und Abrufen von PGP-Schlüsseln einen PGP-Schlüsselserver über LDAPS verwenden.
   - **PGP-Verzeichnis-LDAP:** Wählen Sie diese Option, wenn Sie zum Speichern und Abrufen von PGP-Schlüsseln einen generischen LDAP-Server, wie beispielsweise Netscape Directory Server oder Microsoft Active Directory, verwenden.
   - **PGP-Verzeichnis-LDAPS:** Wählen Sie diese Option, wenn Sie zum Speichern und Abrufen von PGP-Schlüsseln einen generischen LDAPS-Server, wie beispielsweise Netscape Directory Server oder Microsoft Active Directory, verwenden.
   - **X.509-Verzeichnis-LDAP:** Wählen Sie diese Option, wenn Sie zum Speichern und Abrufen von iPlanet CMS oder Microsoft Certificate Services ausgegebenen X.509-Zertifikaten einen generischen LDAP-Verzeichnisserver verwenden.

- **X.509-Verzeichnis-LDAPS:** Wählen Sie diese Option, wenn Sie zum Speichern und Abrufen von iPlanet CMS oder Microsoft Certificate Services ausgegebenen X.509-Zertifikaten einen generischen LDAPS-Verzeichnisserver verwenden.

4. Geben Sie im Feld **Servername** den Domänennamen oder die IP-Adresse des Servers an. Beispiel: server.nai.com oder 123.45.67.89.

5. Geben Sie im Feld **Anschluß** die Anschlußnummer des Servers an. So wird beispielsweise für alte HTTP-Schlüsselserver “11371” verwendet, während für LDAP-Schlüsselserver häufig “389” zum Einsatz kommt.

6. Das Feld **Schlüssel** ist für LDAPS-Server vorgesehen. Der Serverschlüssel wird vom Server zur Authentisierung der Verbindung verwendet. (Die Schlüsseldaten werden erst angezeigt, wenn die Verbindung zum Server hergestellt wurde.)

7. Wählen Sie unter **Serverschlüssel für Domänen** die Option **Beliebige Domäne**, damit PGP aus jeder Domäne Schlüssel an diesen Schlüsselserver senden kann. Diese Option wird standardmäßig aktiviert.

8. Wenn Sie möchten, daß PGP nur von einer bestimmten Domäne aus Schlüssel an diesen Schlüsselserver sendet, wählen Sie die Option unter **Beliebige Domäne**. Geben Sie dann im dafür vorgesehenen Feld den Domänennamen an. Wenn Sie beispielsweise die Domäne “nai.com” festlegen, werden nur die Schlüssel an den Server gesendet, deren E-Mail-Adresse auf nai.com endet.

9. Wählen Sie die Option **In Suchfenster auflisten**, wenn Sie diesen Schlüsselserver im **PGPkeys-Suchfenster** auflisten möchten.

CA-Optionen festlegen

Verwenden Sie die Registerkarte **CA**, um Ihr X.509-Zertifikat Ihrem PGP-Schlüssel hinzuzufügen. Sie müssen jedoch zuerst das Root-CA-Zertifikat vom Schlüsselserver Ihres Unternehmens einholen, bevor Sie Ihr X.509-Zertifikat hinzufügen können. Weitere Anweisungen zum Festlegen von CA-Optionen und zum Hinzufügen Ihres X.509-Zertifikats zu Ihrem Schlüssel erhalten Sie in “PGP-Schlüsseln X.509-Zertifikate hinzufügen” auf Seite 91.

Erweiterte Optionen festlegen

Auf der Registerkarte **Erweitert** können Sie den von Ihnen bevorzugten Verschlüsselungsalgorithmus, die zulässigen Algorithmen, Vertrauensmodelloptionen sowie das Schlüsselexportformat und die Optionen für das automatische Anlegen von Sicherungskopien Ihrer Schlüsselbunde festlegen.

So legen Sie erweiterte Optionen fest:

1. Öffnen Sie das Dialogfeld “PGP-Optionen”, und klicken Sie auf die Registerkarte **Erweitert**.

   Das Dialogfeld “PGP-Optionen” wird mit geöffneter Registerkarte **Erweitert** angezeigt (siehe Abbildung A-6).

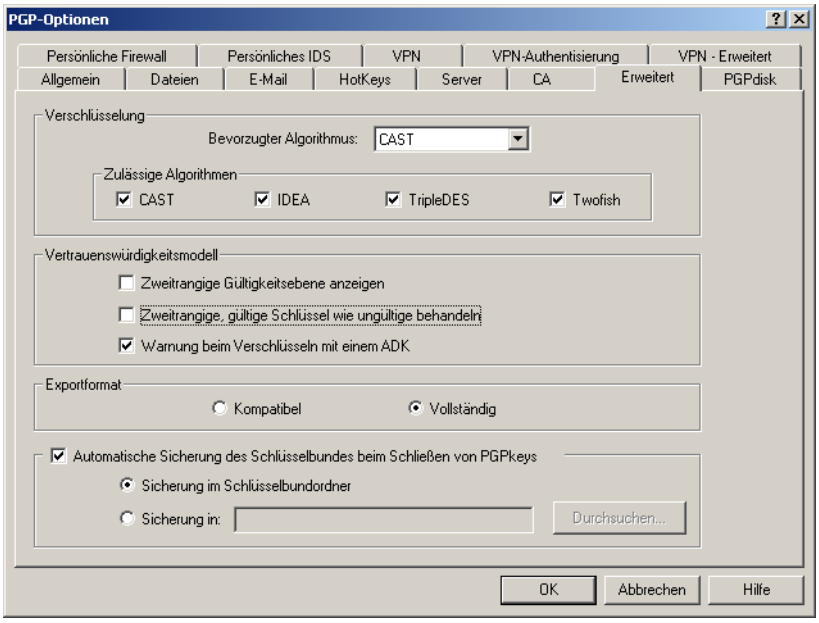


Abbildung A-6. Dialogfeld “PGP-Optionen” (Registerkarte “Erweitert”)

2. Wählen Sie auf der Registerkarte **Erweitert** die gewünschten Verschlüsselungs-, Vertrauensmodell- und Sicherungsoptionen aus. Folgende Optionen stehen zur Verfügung:

Verschlüsselungsalgorithmus

Sie können einen der folgenden Verschlüsselungsalgorithmen für Ihre Verschlüsselungen auswählen:

- **CAST** (Standard)**:** CAST ist eine 128-Bit-Blockverschlüsselung, die mit einem zuverlässigen, für militärische Zwecke geeigneten Verschlüsselungsalgorithmus arbeitet. Dieser ist für seine Fähigkeit bekannt, unberechtigte Zugriffe wirksam zu verhindern.
- **IDEA:** (Wenn Sie IDEA verwenden möchten, müssen Sie diese Festlegung vor dem Erzeugen Ihrer Schlüssel treffen.) IDEA ist der für alle von PGP generierten RSA-Legacy-Schlüssel verwendete Algorithmus.
- **Triple-DES:** (Wenn Sie Triple-DES verwenden möchten, müssen Sie diese Festlegung vor dem Erzeugen Ihrer Schlüssel treffen.) Triple-DES ist ein von der US-Regierung verwendeter Algorithmus, der die Zeit überdauert hat. Dabei handelt es sich um eine Verschlüsselungskonfiguration, in der der DES-Algorithmus dreimal mit drei unterschiedlichen Schlüsseln verwendet wird.
- **Twofish:** Twofish ist ein neuer, von Bruce Schneier entwickelter symmetrischer 256-Bit-Blockverschlüsselungsalgorithmus. Er ist einer von fünf Algorithmen, die vom US-amerikanischen National Institute of Standards and Technology (NIST) als Ersatz für den aktuellen Advanced Encryption Standard (AES) in Betracht gezogen werden.

Weitere Informationen zu diesen Algorithmen finden Sie im Abschnitt “Die symmetrischen Algorithmen von PGP” in der *Einführung in die Kryptographie*.

Die Option **Bevorzugter Algorithmus** wirkt sich wie folgt aus:

- Bei der konventionellen Verschlüsselung wird der bevorzugte Verschlüsselungsalgorithmus verwendet.
- Beim Erstellen eines Schlüssels wird der bevorzugte Verschlüsselungsalgorithmus als Teil des Schlüssels aufgezeichnet, so daß andere Benutzer diesen Algorithmus verwenden, wenn sie für Sie Daten verschlüsseln.

Die Option **Zulässige Algorithmen** wirkt sich wie folgt aus:

- Beim Erstellen eines Schlüssels werden die zulässigen Verschlüsselungsalgorithmen als Teil des Schlüssels aufgezeichnet, so daß andere Benutzer einen dieser Algorithmen verwenden, wenn für Sie der bevorzugte Verschlüsselungsalgorithmus nicht erhältlich ist.

HINWEIS: Die Verschlüsselung mit einem öffentlichen Schlüssel schlägt fehl, wenn die Person, welche die Nachricht verschlüsselt, weder über den bevorzugten noch über einen der zulässigen Verschlüsselungsalgorithmen verfügt.

WARNUNG: Verwenden Sie die Optionen “CAST”, “IDEA”, “Twofish” und “Triple-DES” nur dann, wenn Sie plötzlich erfahren haben, daß ein bestimmter Algorithmus nicht mehr sicher ist. Wenn Sie beispielsweise bemerken, daß Triple-DES von Unbefugten entschlüsselt wurde, können Sie dieses Kontrollkästchen deaktivieren. Alle neu erzeugten Schlüssel werden dann mit einem Datensatz versehen, der besagt, daß Triple-DES beim Verschlüsseln für Sie nicht verwendet werden sollte.

Vertrauenswürdigkeitsmodell

Wenn Sie sich umfassender mit den Themen “Vertrauen” und “Gültigkeit” befassen möchten, finden Sie Informationen dazu in der *Einführung in die Kryptographie.*

PGP gibt Ihnen die Option, das Anzeigen des Vertrauens in Schlüssel zu aktivieren bzw. zu ändern. Außerdem können Sie einstellen, ob Sie vor dem Verschlüsseln einer Nachricht mit einem öffentlichen Schlüssel, zu dem es einen zusätzlichen Entschlüsselungsschlüssel gibt, gewarnt werden möchten oder nicht. Wählen Sie im Bereich “Vertrauensmodell” eine der folgenden Optionen:

- **Zweitrangige Gültigkeitsebene anzeigen:** Aktivieren Sie diese Option, wenn die Schlüssel zweitrangiger Gültigkeitsebene selbst oder die Aktivierung bzw. Deaktivierung der Gültigkeit angezeigt werden sollen. Diese Echtheitsebene wird in Form von Balkensymbolen mit verschiedenen Musterungen angezeigt. Die Aktivierung/Deaktivierung der Gültigkeit wird mit Kreissymbolen dargestellt – grün für “Gültig”, grau für “Ungültig” (Gültigkeit des Schlüssels wurde nicht bestätigt; er wurde weder von einem autorisierten Schlüsselverwalter noch von Ihnen selbst unterzeichnet).
- **Zweitrangige, gültige Schlüssel wie ungültige behandeln:** Wenn Sie diese Option aktivieren, werden alle zweitrangigen, echten Schlüssel wie unechte behandelt. Bei Auswahl dieser Option wird immer, wenn Sie mit zweitrangigen echten Schlüsseln verschlüsseln, das Dialogfeld “PGP-Schlüsselauswahl” angezeigt.
- **Warnung beim Verschlüsseln mit einem ADK:** Durch Aktivieren dieser Option können Sie festlegen, ob beim Verschlüsseln mit einem Schlüssel, mit dem ein Zusätzlicher Entschlüsselungsschlüssel (Additional Decryption Keys, ADK) verknüpft ist, eine Warnung ausgegeben werden soll.

Exportformat

- **Kompatibel:** Exportiert Schlüssel in einem Format, das mit früheren PGP-Versionen kompatibel ist.
- **Vollständig:** Exportiert das neue Schlüsselformat, das Foto-IDs und X.509-Zertifikate enthält.

Automatische Sicherung des Schlüsselbundes beim Schließen von PGPkeys

Aktivieren Sie diese Option, wenn Ihr Schlüsselbund mit öffentlichen und privaten Schlüsseln beim Schließen von PGP automatisch gesichert werden soll.

- **Sicherung im Schlüsselbundordner:** Wählen Sie diese Option, wenn Ihre Schlüsselbund-Sicherungsdateien im Standard-PGP-Schlüsselbundordner gespeichert werden sollen.
- **Sicherung in:** Wählen Sie diese Option, um selbst einen Speicherort für das Speichern Ihrer Sicherungsdateien festzulegen.

3. Klicken Sie auf **OK**, um Ihre Änderungen zu speichern, oder wählen Sie eine andere Registerkarte, um mit dem Konfigurieren Ihrer PGP-Optionen fortzufahren.

Optionen für die persönliche Firewall festlegen

Auf der Registerkarte **Persönliche Firewall** können Sie einen vordefinierten Schutzgrad für Ihre persönliche Firewall auswählen bzw. Ihre eigenen Schutzregeln definieren. Weitere Informationen zu persönlichen Firewalls und zum Festlegen der Optionen dafür finden Sie im Abschnitt “Die persönliche Firewall in PGPnet konfigurieren” auf Seite 202.

Optionen für das persönliche IDS festlegen

Auf der Registerkarte **Persönliches IDS** stehen Ihnen Optionen für die folgenden Aufgaben zur Verfügung:

- Aktivieren des persönlichen Angrifferkennungssystems (IDS)
- Festlegen, ob Sie Angreifer blockieren möchten und wenn ja, wie lange die Kommunikation mit diesen blockiert sein soll
- Festlegen, wie Sie im Falle eines Angriffs gewarnt werden möchten (z. B. per E-Mail oder / und durch Ausgabe eines akustischen Signals)

Weitere Informationen zu Angrifferkennungssystemen und zum Festlegen der Optionen für Ihr persönliches IDS finden Sie im Abschnitt “Das persönliche Angrifferkennungssystem (IDS) in PGPnet konfigurieren” auf Seite 216.

VPN-Optionen festlegen

Auf der Registerkarte **VPN** können Sie die automatische Schlüsselerneuerung steuern und Sie können festlegen, wie Sie mit nicht konfigurierten Hosts kommunizieren möchten.

So legen Sie die VPN-Einstellungen fest:

1. Öffnen Sie das Dialogfeld “PGP-Optionen”, und klicken Sie auf die Registerkarte **VPN**.

   Das Dialogfeld “PGP-Optionen” wird mit geöffneter Registerkarte **VPN** angezeigt (siehe Abbildung A-7).

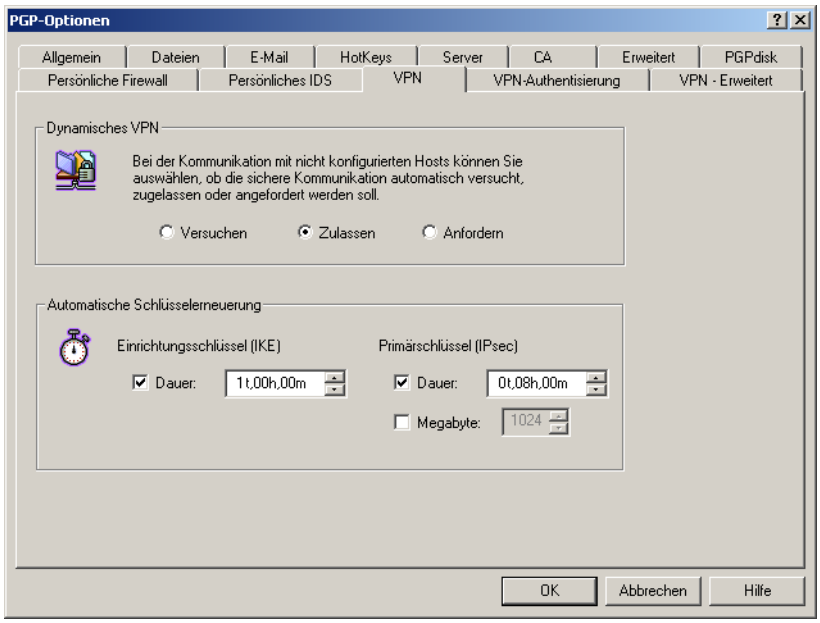


Abbildung A-7. Dialogfeld “PGP-Optionen” (Registerkarte “VPN”)

2. Folgende Optionen stehen zur Verfügung:

Dynamisches VPN

Mit Hilfe der Funktion “Dynamisches VPN” können Sie mit jedem anderen Rechner kommunizieren, auf dem PGPnet installiert ist. Dabei übernimmt PGPnet automatisch die Verschlüsselung sowie die Einrichtung einer SA, ohne daß dazu eine vorherige Konfiguration erforderlich ist. Bei Ihnen muß dazu PGPnet noch nicht einmal ausgeführt werden, es muß lediglich die Option **Versuchen** aktiviert sein.

Stellen Sie sich beispielsweise folgende Situation vor: Auf Ihrem Rechner (Rechner1) und dem Rechner Ihres Kollegen (Rechner2) ist jeweils PGPnet installiert und aktiviert, beide haben die “Dynamisches VPN”-Option “Versuchen” aktiviert, aber keiner von beiden hat den jeweils anderen Rechner konfiguriert (d. h., in Ihrer Hostliste taucht Rechner2 nicht auf, und in der Hostliste des Kollegen taucht Rechner1 nicht auf). Wenn Rechner1 Kontakt zu Rechner2 aufnimmt, erkennt PGPnet, daß Rechner2 IKE unterstützt, und handelt deshalb eine SA aus. Beachten Sie, daß in dem Zeitraum, in dem Rechner1 die Kommunikation mit Rechner2 aufnimmt, und während der SA-Erstellung PGPnet nicht für den Schutz der Kommunikation sorgen kann.

Diese Funktion arbeitet mit dem PGPnetDynamicVPN-Schlüssel, der standardmäßig als Ihr PGPnet-Geräteschlüssel festgelegt ist. Dieser Schlüssel wird von allen verwendet, so daß es nicht zur Authentisierung kommt.

PGPnet verwendet zum Steuern der Kommunikation mit nicht konfigurierten Hosts die drei “Dynamisches VPN”-Optionen **Versuchen**, **Zulassen** und **Anfordern**:

- **Versuchen:** Wenn die Kommunikation mit einem nicht konfigurierten Host gestartet wird (d. h. mit einem Host, der nicht in der Hostliste enthalten ist, so daß auch keine SA vorhanden ist), gestattet PGPnet die Weiterführung der Kommunikation und versucht gleichzeitig, eine SA zu erstellen.

  Wenn es PGPnet nicht gelingt, eine SA auszuhandeln, wird die Kommunikation unsicher fortgesetzt.

  Wenn es PGPnet gelingt, eine SA auszuhandeln, wird die Kommunikation verschlüsselt. Beachten Sie, daß bei der Kommunikation mit unkonfigurierten Hosts einige Pakete unverschlüsselt passieren können, bevor die Verschlüsselung für die Verbindung einsetzt. Diese Verzögerung beträgt im Normalfall etwa eine bis drei Sekunden.

- **Zulassen:** Diese Einstellung ermöglicht anderen Hosts den sicheren Verbindungsaufbau zu Ihrem Computer, Sie initialisieren jedoch keine SAs mit nicht konfigurierten Hosts.

- **Anfordern:** Es wird immer eine sichere Kommunikation angefordert und jeglicher unsichere Verkehr wird unterbunden, falls der Host nicht als unsicherer Host konfiguriert wurde.

VPN-Schlüsselaktualisierung

Sie können Werte für die automatische Schlüsselerneuerung für **Einrichtungsschlüssel (IKE)** und **Primärschlüssel (IPsec)** einstellen. Diese Schlüssel werden für die Erstellung Ihrer Sicherheitsverknüpfungen benötigt. Die Werte für die Einrichtungsschlüssel (IKE) können zeitlich festgelegt werden (**Dauer**); die Werte für Primärschlüssel (IPsec) können zeitlich (**Dauer**) oder nach Datengröße (**Megabyte**) festgelegt werden.

- **Dauer** wird auf die folgende Art und Weise dargestellt:

  2t, 08h, 04m (Schlüssel läuft in 2 Tagen, 8 Stunden und 4 Minuten ab)

- **Megabyte** wird auf die folgende Art und Weise dargestellt:

  99 (Schlüssel läuft nach einer Datenübertragung von 99 MB ab)

Beachten Sie folgendes: Wenn Sie eine SA mit einem anderen Host herstellen, verwendet PGPnet den jeweils niedrigeren Schlüsselerneuerungswert der beiden Hosts. Folglich wird eine SA möglicherweise ungültig, bevor der Erneuerungswert erreicht wird.

WARNUNG: Durch das Verringern des Megabyte-Standardwerts kommt es bei der Übertragung großer Dateien möglicherweise zu einer mehrfachen, erneuten Schlüsselerstellung. Dies kann wiederum zu einer vorübergehenden Unterbrechung der normalen Netzwerkfunktion führen.

---

3. Klicken Sie auf **OK**, um Ihre Änderungen zu speichern, oder wählen Sie eine andere Registerkarte, um mit dem Konfigurieren Ihrer PGP-Optionen fortzufahren.

Werte für die automatische Schlüsselerneuerung festlegen

So ändern Sie die Werte für die automatische Erneuerung der Einrichtungsschlüssel (IKE):

1. Öffnen Sie die Registerkarte **VPN** (**Ansicht—>Optionen**). Im unteren Abschnitt der **PGPnet**-Registerkarte **VPN** werden die Angaben für die **Automatische Schlüsselerneuerung** angezeigt.
2. Mit den Auf- und Abwärtspfeilen neben dem Feld “Dauer” können Sie den entsprechenden Zeitraum festlegen oder einen numerischen Wert in folgende Felder eingeben: t, h, m.
3. Klicken Sie auf **OK**.

So legen Sie die Werte für die automatischen Erneuerung der Primärschlüssel (IPsec) fest:

1. Öffnen Sie die Registerkarte **VPN** (**Ansicht—>Optionen**). Im unteren Abschnitt der **PGPnet**-Registerkarte **VPN-Optionen** werden die Angaben für die **Automatische Schlüsselerneuerung** angezeigt.
2. Um die Dauer für einen Primärschlüssel festzulegen, klicken Sie auf **Dauer**. Mit den Auf- und Abwärtspfeilen neben dem Feld **Dauer** können Sie den entsprechenden Zeitraum einstellen oder einen numerischen Wert in den folgenden Feldern eingeben: t, h, m.

3. Um einen Datenwert in **Megabyte** für Primärschlüssel festzulegen, klicken Sie auf das Feld neben **Megabyte**. Mit den Auf- und Abwärtspfeilen können Sie die entsprechende Megabyte-Begrenzung festlegen oder einen numerischen Wert eingeben.
4. Klicken Sie auf **OK**.

Optionen für die VPN-Authentisierung festlegen

Auf der Registerkarte **VPN-Authentisierung** können Sie folgende Aufgaben ausführen:

- Wählen Sie einen PGP-Schlüssel aus, um Ihren lokalen Rechner zu authentisieren (**PGP-Authentisierung**).
- Wählen Sie ein X.509-Zertifikat aus, um Ihren lokalen Rechner zu authentisieren (**X.509-Authentisierung**).
- Entfernte Authentisierung steuern.

So legen Sie die Optionen für die VPN-Authentisierung fest:

1. Öffnen Sie das Dialogfeld “PGP-Optionen”, und klicken Sie auf die Registerkarte **VPN-Authentisierung**.

   Das Dialogfeld “PGP-Optionen” wird mit geöffneter Registerkarte **VPN-Authentisierung** angezeigt (siehe Abbildung A-8).

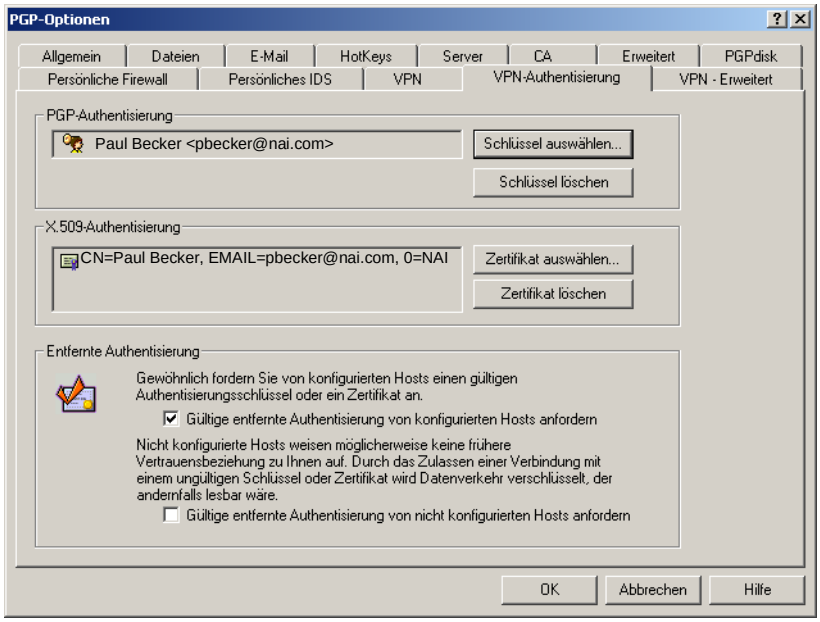


Abbildung A-8. Dialogfeld “PGP-Optionen” (Registerkarte “VPN-Authentisierung”)

2. So legen Sie Ihre Optionen für die VPN-Authentisierung fest:

Verbindungen authentisieren

- **Schlüssel auswählen:** Zeigt ein Dialogfeld an, in dem Sie Ihr Schlüsselpaar auswählen können. Sie werden danach aufgefordert, die Paßphrase für den ausgewählten Schlüssel einzugeben.
- **Schlüssel löschen:** Löscht den ausgewählten Schlüssel.
- **Zertifikat auswählen.** Zeigt ein Dialogfeld an, in dem Sie Ihr X.509-Zertifikat am Schlüsselbund auswählen können. Sie werden aufgefordert, die Paßphrase für das ausgewählte Zertifikat einzugeben.
- **Zertifikat löschen:** Löscht das ausgewählte X.509-Zertifikat.

Wenn Sie auf **OK** klicken, werden Sie zur Eingabe der Paßphrase für den ausgewählten Authentisierungsschlüssel oder das -zertifikat aufgefordert. Geben Sie die Paßphrase ein, und klicken Sie auf **OK**. Sie werden bei jeder Anmeldung bei PGPnet zur Eingabe dieser Paßphrase aufgefordert.

Entfernte Authentisierung

Normalerweise werden Sie von konfigurierten Hosts einen gültigen Schlüssel oder ein Zertifikat zur Authentisierung anfordern. Klicken Sie dazu auf **Gültige entfernte Authentisierung von konfigurierten Hosts anfordern**.

Zwischen Ihnen und diesen nicht konfigurierten Hosts hat möglicherweise noch keine Vertrauensbeziehung bestanden. Wenn ihnen der Verbindungsaufbau mit einem ungültigen Schlüssel bzw. einem ungültigen Zertifikat gestattet wird, erfolgt die Verschlüsselung des Verkehrs, der ansonsten unverschlüsselt ablaufen würde.

- Wenn Verbindungen von nicht konfigurierten Hosts mit einem ungültigen Schlüssel bzw. einem ungültigen Zertifikat trotzdem zugelassen werden sollen, müssen Sie die Option **Gültige entfernte Authentisierung von nicht konfigurierten Hosts anfordern** deaktivieren.
- Wenn dagegen von unkonfigurierten Hosts eine gültige entfernte Authentisierung angefordert werden soll, aktivieren Sie die Option **Gültige entfernte Authentisierung von nicht konfigurierten Hosts anfordern**.

3. Klicken Sie auf **OK**, um Ihre Änderungen zu speichern, oder wählen Sie eine andere Registerkarte, um mit dem Konfigurieren Ihrer PGP-Optionen fortzufahren.

Optionen auf der Registerkarte “VPN – Erweitert” festlegen

WARNUNG: Die Standardeinstellungen auf dieser Registerkarte ermöglichen die Kommunikation mit PGPnet oder Benutzern der starken Verschlüsselung GVPN. Sie sollten die Einstellungen nur ändern, wenn Sie ein erfahrener IPsec-Benutzer sind.

Die Registerkarte **VPN - Erweitert** (**Ansicht—>Optionen**) enthält die Optionen **Zulässige entfernte Vorschläge** und IKE- und IPsec-**Vorschläge**.

- Mit den Optionen im Abschnitt **Zulässige entfernte Vorschläge** wird PGPnet angewiesen, alle Vorschläge von anderen Benutzern zu akzeptieren, die ein in diesen Feldern aktiviertes Element enthalten. Davon ausgenommen ist die Einstellung **Keine** für die Optionen **Chiffrierungen** und **Hashes**. Die Einstellung **Keine** sollte, wenn überhaupt, nur mit größter Vorsicht verwendet werden. Falls Sie für **Chiffrierungen** (Verschlüsselung) die Einstellung **Keine** festlegen, akzeptiert PGPnet Vorschläge, die keine Verschlüsselung aufweisen. Falls Sie für **Hashes** (Authentisierung) die Einstellung **Keine** festlegen, akzeptiert PGPnet Vorschläge, die keine Authentisierung aufweisen.
- In den Abschnitten **IKE-Vorschläge** und **IPsec-Vorschläge** sind die Vorschläge aufgeführt, die Sie anderen unterbreiten. Andere Benutzer müssen mindestens einen der Vorschläge für IKE und IPsec genau wie angegeben akzeptieren.

So legen Sie die Optionen auf der Registerkarte “VPN – Erweitert” fest:

1. Öffnen Sie das Dialogfeld “PGP-Optionen”, und klicken Sie auf die Registerkarte **VPN – Erweitert**.

   Das Dialogfeld “PGP-Optionen” wird mit geöffneter Registerkarte **VPN – Erweitert** angezeigt (siehe Abbildung A-9 auf Seite 271).

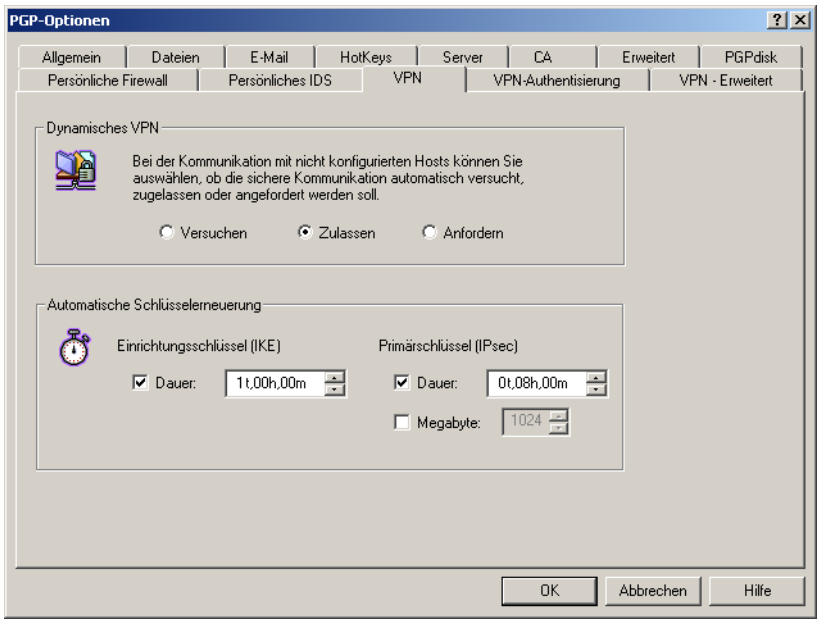


Abbildung A-9. Dialogfeld “PGP-Optionen” (Registerkarte “VPN – Erweitert”)

2. Auf dieser Registerkarte stehen die folgenden Optionen zur Verfügung:

Zulässige entfernte Vorschläge

Im Abschnitt **Zulässige entfernte Vorschläge** dieser Registerkarte werden die in PGPnet zulässigen Typen von Chiffrierungen, Hashes, Komprimierung und Diffie-Hellman-Schlüsseln aufgeführt.

HINWEIS: Die Einstellungen auf dieser Registerkarte sollten nur von erfahrenen IPsec-Benutzern geändert werden.

- **Chiffrierungen:** Chiffrierungen sind zur Ver- und Entschlüsselung verwendete Algorithmen. Um eine bestimmte Art von Chiffrierung (CAST oder TripleDES) verwenden zu können, müssen Sie die Optionen links neben der jeweiligen Chiffrierung aktivieren. Die Einstellung “Keine” sollte, wenn überhaupt, nur mit größter Vorsicht verwendet werden, da PGPnet angewiesen wird, Vorschläge von anderen Benutzern zu akzeptieren, die keine Verschlüsselung aufweisen.
- **Hashes**: Eine Hash-Funktion verwendet eine Eingabezeichenkette beliebiger Länge und konvertiert diese in eine Ausgabezeichenkette mit fester Länge. Um eine bestimmte Art von Hash (SHA-1 oder MD5) verwenden zu können, müssen Sie das Kontrollkästchen links neben der Hash-Funktion markieren. Die Einstellung “Keine” sollte, wenn überhaupt, nur mit größter Vorsicht bzw. überhaupt nicht verwendet werden, da PGPnet angewiesen wird, Vorschläge von anderen Benutzern zu akzeptieren, die keine Verschlüsselung aufweisen.
- **Diffie-Hellman**: Diffie-Hellman ist ein Schlüsselvereinbarungsprotokoll. Um eine bestimmte Art von Schlüsselgröße (1024 oder 1536) verwenden zu können, müssen Sie das Feld links neben der Schlüsselgröße markieren.
- **Komprimierung**: Eine Komprimierungsfunktion verwendet eine Eingabe fester Länge und gibt eine kürzere Ausgabe mit fester Länge aus. Es gibt zwei unterschiedliche Komprimierungsarten: “LZS” und “Entkomprimieren”. Markieren Sie das Feld links neben dem Komprimierungstyp, um eine bestimmte Art der Komprimierung zuzulassen.

HINWEIS: Mit “LZS” und “Entkomprimieren” wird die Leistung von Kommunikationsgeräten mit niedriger Geschwindigkeit (beispielsweise Modems oder ISDN) gesteigert. Die Leistung von Kommunikationsgeräten mit hoher Geschwindigkeit (beispielsweise Kabelmodem, DSL, T-1 und T-3) wird hierdurch hingegen gemindert. Dies ist auf den Overhead der Komprimierungsroutinen zurückzuführen.

Anweisungen dazu, wie Sie zulässige entfernte Vorschläge hinzufügen und entfernen können, finden Sie im Abschnitt “Zulässige entfernte Vorschläge hinzufügen und entfernen” auf Seite 276.

Vorschläge

Mit den Optionen im Abschnitt **Vorschläge** der Registerkarte **VPN – Erweitert** können Sie Vorschläge hinzufügen, bearbeiten, entfernen und neu anordnen. Die IKE- und IPsec-Vorschläge informieren PGPnet darüber, welche Vorschläge anderen Benutzern vorgelegt werden sollen. Die Vorschläge müssen genau wie angegeben akzeptiert werden. Beachten Sie, daß die Mindestzahl von IKE- und IPsec-Vorschlägen bei 1 und die Höchstzahl bei 16 liegt.

HINWEIS: Nur erfahrene IPsec-Benutzer sollten auf dieser Registerkarte Änderungen vornehmen.

In IKE-Vorschlägen werden folgende Informationsarten verwendet:

- **Authentisierung:** Die Authentisierung dient zum Verifizieren von Informationen, wie beispielsweise der Identität. Es gibt drei Arten der Authentisierung: Schlüsselteil (ein geheimer Schlüssel wird von zwei oder mehr Benutzern gemeinsam verwendet), DSS-Unterschrift (eine Unterschrift gemäß dem Digital Signature Standard) und RSA-Unterschrift.
- **Hash:** Eine Hash-Funktion verwendet eine Eingabezeichenkette beliebiger Länge und konvertiert diese in eine Ausgabezeichenkette mit fester Länge. Es gibt folgende zwei Hash-Arten: SHA (Secure Hash Algorithm) und MD5 (Message-Digest Algorithm).
- **Chiffrierung:** Chiffrierungen sind zur Ver- und Entschlüsselung verwendete Algorithmen. Folgende zwei Arten stehen zur Verfügung: CAST und TripleDES.
- **DH (Diffie-Hellman):** Diffie-Hellman ist ein Schlüsselvereinbarungsprotokoll. Folgende zwei Größen von Diffie-Hellman-Schlüsseln stehen zur Verfügung: 1024 und 1536.

In IPsec-Vorschlägen werden folgende Informationsarten verwendet:

- **AH:** Aktiviert die Authentisierungs-Header (AH). AH wird zur Gewährleistung der Abwärtskompatibilität mit älteren IPsec-Produkten verwendet. AH bietet keine Verschlüsselung. AH authentisiert Ihre IP-Adressen. Das kann jedoch zu Problemen führen. Da Ihre IP-Adressen von NAT übersetzt werden, kann die von AH durchgeführte Authentisierung Ihrer IP-Adresse zu einem Fehler bei der Paketauthentisierung führen.

  Um AH verwenden zu können, müssen Sie auf der Registerkarte **VPN – Erweitert** für **Chiffrierungen** die Einstellung **Keine** wählen, einen IPsec-Vorschlag hinzufügen, der AH enthält, und diesen Vorschlag an die oberste Position der Vorschlagliste verschieben.

  Folgende zwei Arten stehen zur Verfügung: SHA und MD5.

- **ESP:** Aktiviert ESP (Encapsulating Security Payload), ein Unterprotokoll von IPsec für die Verschlüsselung und Authentisierung.

  Um externen Vorschlägen die Initialisierung von ESP **None** zu erlauben, müssen Sie auf der Registerkarte **VPN – Erweitert** für **Chiffrierungen** die Einstellung **Keine** festlegen. Außerdem müssen Sie Ihren IPsec-Vorschlägen einen Vorschlag hinzufügen, der ESP None enthält, und diesen Vorschlag an die oberste Position der Vorschlagliste verschieben.

  Es gibt drei verschiedene Hash-Arten: Keine, SHA und MD5. Es gibt drei verschiedene Chiffrierungsarten: Keine, CAST und TripleDES.

- **IPPCP:** Aktiviert das Protokoll IPPCP (IP Payload Compression Protocol). Verwenden Sie dies nur für DFÜ-Verbindungen. Es beansprucht umfangreichen Overhead.

  Um IPPCP verwenden zu können, müssen Sie auf der Registerkarte **VPN – Erweitert** einen neuen IPsec-Vorschlag mit IPPCP erstellen, diesen Vorschlag an die oberste Position der Vorschlagliste verschieben und **IPPCP** und **LZS** oder **Entkomprimieren** aktivieren. Entkomprimieren beansprucht einen viel größeren Overhead als LZS, weshalb LZS empfohlen wird.

  Die Komprimierungsalgorithmen erfordern eine Eingabe fester Länge und führen zu einer kleineren Ausgabe fester Länge.

Wenn PGPnet von einem anderen Rechner IPPCP vorgeschlagen wird, akzeptiert PGPnet diesen Vorschlag, sofern die Optionen **LZS** und **Entkomprimieren** im Abschnitt **Zulässige entfernte Vorschläge** der Registerkarte **VPN – Erweitert** nicht deaktiviert sind.

Es gibt zwei IPPCP-Arten: Entkomprimieren und LZS.

HINWEIS: Durch "LZS" und "Entkomprimieren" wird die Leistung von Kommunikationsgeräten mit niedriger Geschwindigkeit (wie z. B. Modems und ISDN) erhöht, die Leistungsfähigkeit von Kommunikationsgeräten mit hoher Geschwindigkeit hingegen (beispielsweise Kabelmodems, DSL, T-1 und T-3) wird hierdurch gemindert. Dies ist auf den Overhead der Komprimierungsroutinen zurückzuführen.

Anweisungen dazu, wie Sie IKE- und IPsec-Vorschläge hinzufügen, bearbeiten, neu anordnen und entfernen können, finden Sie im Abschnitt "Mit IKE- und IPsec-Vorschlägen arbeiten" auf Seite 276.

Höchste Geheimhaltung beim Weiterleiten

Für sämtliche IPsec-Vorschläge wird dieselbe Diffie-Hellman-Einstellung für die **Höchste Geheimhaltung beim Weiterleiten** verwendet: **Keine**, **1024** oder **1536** Bits.

Wenn die Option **Höchste Geheimhaltung beim Weiterleiten** aktiviert ist, erzeugt PGPnet die Schlüssel für eine bestimmte Verbindung und beseitigt dann das zur Erzeugung dieses Schlüssels verwendete Material.

Falls ein Angreifer eine bestimmte SA nach dem Brechstangenprinzip angreift, würde es ihm nichts nützen, eine frühere oder spätere Verbindung anzugreifen.

Wenn PFS aktiviert ist (wenn Sie also **1024** oder **1536** wählen), muß es auf allen Rechnern aktiviert sein, mit denen Sie kommunizieren.

PFS erfordert zusätzliche Austauschvorgänge von Diffie-Hellman-Schlüsseln, was zu zusätzlicher Verarbeitungszeit führt. Das kann bei Gateways zum Problem werden, die hunderte SA-Abstimmungen pro Minute verarbeiten müssen, wenn jeder PFS verwendet.

Wenn PFS auf Ihrem Rechner aktiviert und auf einem Gateway deaktiviert ist, ist keine SA-Abstimmung mit diesem Gateway möglich.

Schaltfläche “Standardeinstellungen”

Mit dieser Schaltfläche stellen Sie die Standardeinstellungen für alle Felder in diesem Bildschirm wieder her. In den meisten Fällen reichen die Standardeinstellungen zur Erstellung von SAs und zur Verwendung von PGPnet aus.

3. Klicken Sie auf **OK**, um Ihre Änderungen zu speichern, oder wählen Sie eine andere Registerkarte, um mit dem Konfigurieren Ihrer PGP-Optionen fortzufahren.

Zulässige entfernte Vorschläge hinzufügen und entfernen

So fügen Sie ein Element zu “Zulässige entfernte Vorschläge” hinzu:

1. Öffnen Sie das Dialogfeld “PGP-Optionen” (**Ansicht—>Optionen**).
2. Klicken Sie auf die Registerkarte **VPN – Erweitert**.
3. Markieren Sie das Kontrollkästchen links neben dem Element.
4. Klicken Sie auf **OK**.

So entfernen Sie ein Element aus “Zulässige entfernte Vorschläge”:

1. Öffnen Sie das Dialogfeld “PGP-Optionen” (**Ansicht—>Optionen**).
2. Klicken Sie auf die Registerkarte **VPN – Erweitert**.
3. Heben Sie die Markierung des Kontrollkästchens links neben dem Element auf.
4. Klicken Sie auf **OK**.

Mit IKE- und IPsec-Vorschlägen arbeiten

So fügen Sie einen IKE- oder IPsec-Vorschlag hinzu:

1. Öffnen Sie das Dialogfeld “PGP-Optionen” (**Ansicht—>Optionen**).
2. Klicken Sie auf die Registerkarte **VPN – Erweitert**.
3. Klicken Sie auf **Neu**, und wählen Sie **IKE-Vorschlag** oder **IPsec-Vorschlag**.
4. Legen Sie im Dialogfeld “IKE-Vorschlag” bzw. “IPsec-Vorschlag” die gewünschten Einstellungen fest (siehe Abbildung A-10 auf Seite 277).

“IKE-Vorschlag” (Beispiel)

“IPsec-Vorschlag” (Beispiel)

Abbildung A-10. Dialogfelder “IKE-Vorschlag” und “IPsec-Vorschlag”

5. Klicken Sie auf **OK**.
6. Wenn Sie einen IPsec-Vorschlag hinzufügen, wählen Sie für die Option **Höchste Geheimhaltung beim Weiterleiten** die entsprechende Diffie-Hellman-Einstellung (**Keine**, **1024** oder **1536**) aus. Für sämtliche IPsec-Vorschläge wird dieselbe Diffie-Hellman-Einstellung verwendet.
7. Klicken Sie auf **OK**.

So bearbeiten Sie einen IKE- oder IPsec-Vorschlag:

1. Öffnen Sie das Dialogfeld “PGP-Optionen” (**Ansicht—>Optionen**).
2. Klicken Sie auf die Registerkarte **VPN – Erweitert**.
3. Wählen Sie den jeweiligen Vorschlag aus.
4. Klicken Sie auf **Bearbeiten**.
5. Nehmen Sie im Dialogfeld “IKE-Vorschlag” bzw. “IPsec-Vorschlag” die gewünschten Änderungen vor (siehe Abbildung A-10).
6. Klicken Sie auf **OK**.
7. Überprüfen Sie die Einstellung, die im Feld **Höchste Geheimhaltung beim Weiterleiten** angezeigt wird. Beachten Sie, daß für sämtliche IPsec-Vorschläge dieselbe Diffie-Hellman-Einstellung verwendet wird. Ändern Sie die Einstellung gegebenenfalls.
8. Klicken Sie auf der Registerkarte **VPN – Erweitert** auf **OK**.

So entfernen Sie einen IKE- oder IPsec-Vorschlag:

1. Öffnen Sie das Dialogfeld “PGP-Optionen” (**Ansicht—>Optionen**).
2. Klicken Sie auf die Registerkarte **VPN – Erweitert**.
3. Klicken Sie auf den jeweiligen Vorschlag.
4. Klicken Sie auf **Entfernen**.
5. Klicken Sie auf **OK**.

So ordnen Sie IKE- oder IPsec-Vorschläge neu an:

1. Öffnen Sie das Dialogfeld “PGP-Optionen” (**Ansicht—>Optionen**).
2. Klicken Sie auf die Registerkarte **VPN – Erweitert**.
3. Wählen Sie den jeweiligen Vorschlag aus.
4. Klicken Sie auf **Nach Oben**, um den Vorschlag nach oben zu verschieben. Klicken Sie auf **Nach Unten**, um den Vorschlag nach unten zu verschieben.
5. Klicken Sie auf **OK**.

PGPdisk-Optionen festlegen

Auf der Registerkarte **PGPdisk** können Sie festlegen, wie die vorhandenen Volumes entladen werden sollen.

So legen Sie PGPdisk-Optionen fest:

1. Öffnen Sie das Dialogfeld “PGP-Optionen”, und klicken Sie auf die Registerkarte **PGPdisk**.

   Das Dialogfeld “PGP-Optionen” wird mit geöffneter Registerkarte **PGPdisk** angezeigt (siehe Abbildung A-11).

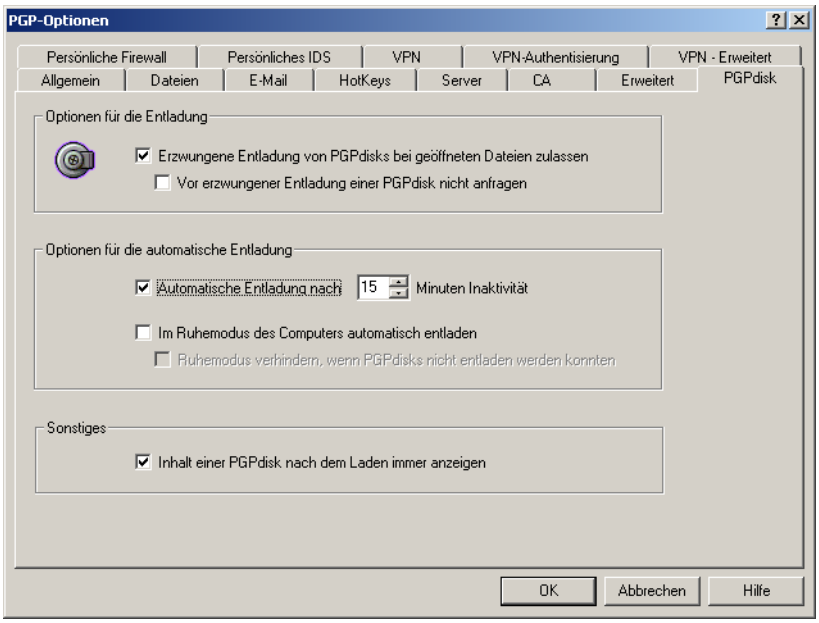


Abbildung A-11. Dialogfeld “PGP-Optionen” (Registerkarte “PGPdisk”)

2. Wählen Sie die gewünschten Optionen, indem Sie auf die entsprechenden Registerkarten klicken und dort die jeweiligen Kontrollkästchen markieren.

Optionen für die Entladung

- **Erzwungene Entladung von PGPdisks bei geöffneten Dateien zulassen:** Wenn diese Option aktiviert ist, können PGPdisk-Volumes selbst bei noch geöffneten Dateien entladen werden. Mit Hilfe einer Warnung wird darauf hingewiesen, daß in diesem Fall Daten verlorengehen können.

  Mit der Option **Vor erzwungener Entladung einer PGPdisk nicht anfragen** können Sie festlegen, daß PGPdisk PGPdisk-Volumes automatisch entlädt, ohne Sie über möglicherweise noch geöffnete Dateien zu informieren.

WARNUNG: Beim Entladen von PGPdisk-Volumes, bei denen noch Dateien geöffnet sind, können Daten verlorengehen. Wird die Option **Erzwungene Entladung von PGPdisks bei geöffneten Dateien zulassen** aktiviert, erscheint eine Warnmeldung, wenn in dem PGPdisk-Volume, das entladen werden soll, noch Dateien geöffnet sind. Wenn Sie die Option **Vor erzwungener Entladung einer PGPdisk nicht anfragen** wählen, wird diese Warnung nicht angezeigt.

Optionen für die automatische Entladung

Die Einstellungen zum automatischen Entladen sind hilfreich, wenn Sie Ihren Computer für eine bestimmte Zeit unbeaufsichtigt lassen müssen. Sie müssen die Zeitangaben für diese Einstellungen in Abhängigkeit davon einrichten, wie sicher Ihr System vor unbefugtem Zugriff ist. Es ist möglich, beide Optionen gleichzeitig festzulegen.

- **Automatische Entladung nach [15] Minuten Inaktivität:** Ist diese Option aktiviert, entlädt PGPdisk automatisch alle verbundenen PGPdisk-Volumes, wenn Ihr Computer so viele Minuten inaktiv ist, wie im Feld angezeigt wird. Als Inaktivitätszeitraum kann jeder Wert von 1 bis 999 Minuten festgelegt werden.

HINWEIS: PGPdisk kann ein PGPdisk-Volume nicht automatisch entladen, wenn Dateien in diesem Volume geöffnet sind, es sei denn, Sie haben sowohl die Option **Erzwungene Entladung von PGPdisks bei geöffneten Dateien zulassen** als auch die Option **Vor erzwungener Entladung einer PGPdisk nicht anfragen** aktiviert.

- **Im Ruhemodus des Computers automatisch entladen:** Ist diese Option aktiviert, entlädt PGPdisk automatisch alle geladenen PGPdisk-Volumes, wenn Ihr Computer in den Standby-Modus geschaltet wird. (Nicht alle Computer-Modelle verfügen über einen Standby-Modus.)

  Mit der Option **Ruhemodus verhindern, wenn PGPdisks nicht entladen werden konnten** wird gewährleistet, daß Ihr Computer nicht in den Standby-Modus schaltet, wenn ein PGPdisk-Volume nicht entladen werden kann.

HINWEIS: Diese beiden Optionen (**Im Ruhemodus des Computers automatisch entladen** und **Ruhemodus verhindern, wenn PGPdisks nicht entladen werden konnten**) sind unter Windows NT nicht verfügbar.

Sonstiges

- **Inhalt einer PGPdisk nach dem Laden immer anzeigen**: Wenn diese Option aktiviert ist, öffnet sich nach dem Laden des PGPdisk-Volumes ein neues Windows-Explorer-Fenster, in dem der Inhalt des geladenen PGPdisk-Volumes angezeigt wird.

3. Klicken Sie auf **OK**, wenn Sie alle Einstellungen festgelegt haben.

Problembehebung in PGP B

Dieser Anhang enthält Informationen zu Problemen, die bei der Arbeit mit PGP möglicherweise auftreten, sowie entsprechende Lösungsvorschläge. In der folgenden Tabelle haben wir die PGP-Fehlermeldungen, mögliche Ursachen und Vorschläge zur Behebung des Fehlers zusammengestellt.

Fehlermeldung	Ursache	Lösung
Die Datei mit den Verwaltungseinstellungen konnte nicht gefunden werden	Die Datei mit den Einstellungen, die die vom PGP-Administrator (hierbei handelt es sich üblicherweise um einen Mitarbeiter der IS/IT-Abteilung) eingerichtete Konfiguration enthält, ist nicht vorhanden.	Installieren Sie PGP erneut auf Ihrem Rechner. Falls die Meldung daraufhin noch immer angezeigt wird, wenden Sie sich an den PGP-Administrator, und informieren Sie ihn über den Inhalt dieser Meldung. Es muß ein neues PGP-Installationsprogramm für Sie erzeugt werden.
Authentisierung durch entfernte SKEP-Verbindung abgewiesen	Der Benutzer auf der entfernten Seite der Netzwerkverbindung für die Schlüsselteildatei hat den Schlüssel abgewiesen, den Sie zur Authentisierung bereitgestellt haben.	Verwenden Sie einen anderen Schlüssel zur Authentisierung der Schlüsselteil-Netzwerkverbindung, bzw. versichern Sie dem entfernten Benutzer, daß der von Ihnen verwendete Schlüssel gültig ist.
Der PGP-Treiber zum Sperren von Speicherseiten funktioniert nicht korrekt.	Als Ursache kommen eine falsche Installation, ein Systemausfall oder Manipulationen an Ihrem System durch Unbefugte in Frage.	Installieren Sie PGP neu.
Der gewünschte Vorgang kann nicht ausgeführt werden, da der Ausgabepuffer zu klein ist.	Die Ausgabe ist für die internen Puffer zu groß.	Beim Verschlüsseln oder Unterschreiben müssen Sie möglicherweise die Nachricht aufteilen und immer nur kleinere Abschnitte verschlüsseln bzw. unterschreiben. Wenn Sie entschlüsseln oder verifizieren, bitten Sie den Absender, Ihnen kleinere verschlüsselte bzw. unterschriebene Teile zu senden.

Fehlermeldung	Ursache	Lösung
Der angegebene Schlüssel kann nur für Unterschriften verwendet werden. Die Verschlüsselung war daher nicht möglich.	Der ausgewählte Schlüssel kann nur zum Unterschreiben verwendet werden.	Wählen Sie einen anderen Schlüssel aus, oder erstellen Sie einen neuen Schlüssel, mit dem Daten verschlüsselt werden können.
Der angegebene Schlüssel kann nur zur Verschlüsselung verwendet werden. Die Unterschrift war daher nicht möglich.	Der ausgewählte Schlüssel kann nur zum Verschlüsseln verwendet werden.	Wählen Sie einen anderen Schlüssel aus, oder erstellen Sie einen neuen Schlüssel, mit dem Daten unterschrieben werden können.
Fehler in DNS	Die angegebene Zieladresse ist nicht korrekt, oder die Netzwerkverbindung ist nicht richtig konfiguriert.	Stellen Sie sicher, daß die von Ihnen angegebene Zieladresse korrekt ist. Wenn dies der Fall ist, überprüfen Sie Ihre Verbindung zum Netzwerk.
Identische Schlüsselteile können nicht kombiniert werden	Sie versuchen, dieselben Schlüsselteile zweimal zu kombinieren.	Wenn Sie die Schlüsselteile über eine Schlüsselteildatei erhalten haben, wählen Sie nach Möglichkeit eine andere Schlüsselteildatei. Falls die Schlüsselteile aus einem Netzwerk stammen, müssen Sie den Benutzer am entfernten Ort bitten, einen anderen Satz von Schlüsselteilen zu senden.
In Ihrem Schlüsselbund konnten keine geheimen Schlüssel gefunden werden.	Es gibt keine privaten Schlüssel an Ihrem Schlüsselbund.	Erzeugen Sie in PGPkeys Ihr eigenes Schlüsselpaar.
Socket nicht verbunden	Die Netzwerkverbindung zum PGP-Schlüsselserver oder die Netzwerkverbindung für die Schlüsselteildatei ist abgebrochen.	Stellen Sie die Verbindung nach Möglichkeit erneut her, indem Sie das zuvor zum Starten der Verbindung verwendete Verfahren wiederholen. Sollte dies fehlschlagen, überprüfen Sie die Verbindung zum Netzwerk.
Die Aktion konnte aufgrund eines ungültigen Dateivorgangs nicht ausgeführt werden.	Daten konnten nicht gelesen oder in eine bestimmte Datei geschrieben werden.	Die Datei ist wahrscheinlich fehlerhaft. Versuchen Sie gegebenenfalls, die PGP-Voreinstellungen so zu ändern, daß eine andere Datei verwendet wird.

Fehlermeldung	Ursache	Lösung
Die Bewertungszeit zur PGP-Verschlüsselung und Unterschriften ist abgelaufen. Der Vorgang wurde abgebrochen.	Die Produktbewertungszeit ist abgelaufen.	Laden Sie die Freeware-Version herunter, oder kaufen Sie das Produkt im Handel.
Der Schlüsselbund enthält ein fehlerhaftes PGP-Paket.	Die PGP-Nachricht, mit der Sie arbeiten, oder der Schlüsselbund ist fehlerhaft.	Bitten Sie den Absender, die Nachricht erneut zu senden, falls es eine Nachricht ist, mit der Sie arbeiten. Falls es sich um Ihren eigenen Schlüsselbund handelt, stellen Sie ihn von der Sicherungskopie des Schlüsselbundes wieder her.
Die Schlüsselbunddatei ist fehlerhaft.	Daten konnten nicht gelesen oder in eine bestimmte Datei geschrieben werden.	Eine Datei ist wahrscheinlich fehlerhaft oder nicht vorhanden. Dabei kann es sich um die Schlüsselbunddatei handeln oder auch nicht. Verwenden Sie nach Möglichkeit einen anderen Dateinamen oder -pfad.
Die Nachricht/Daten enthält/enthalten eine separate Unterschrift.	Die Unterschrift für die Nachricht/Datei befindet sich in einer separaten Datei.	Doppelklicken Sie zuerst auf die separate Unterschriftendatei.
Die eingegebene Paßphrase stimmt nicht mit der Paßphrase des Schlüssels überein.	Die eingegebene Paßphrase ist falsch.	Sie haben möglicherweise die Feststelltaste gedrückt oder die Paßphrase falsch geschrieben. Versuchen Sie es erneut.
In der PGP-Bibliothek ist nicht genügend Speicherplatz.	Im Betriebssystem steht nicht mehr genügend Arbeitsspeicher zur Verfügung.	Schließen Sie andere aktive Programme. Falls dadurch das Problem nicht behoben wird, benötigt Ihr Computer möglicherweise mehr Arbeitsspeicher.
Die angegebene Benutzer-ID ist in dem ausgewählten Schlüssel bereits vorhanden. Sie wurde daher nicht hinzugefügt.	Sie können einem Schlüssel keine Benutzer-ID hinzufügen, wenn bereits eine entsprechende ID auf dem Schlüssel existiert.	Fügen Sie eine andere Benutzer-ID hinzu, oder löschen Sie zuerst die passende.
Der angegebene Schlüssel konnte in Ihrem Schlüsselbund nicht gefunden werden.	Der zum Entschlüsseln der aktuellen Nachricht benötigte Schlüssel befindet sich nicht an Ihrem Schlüsselbund.	Bitten Sie den Absender der Nachricht, die Nachricht erneut zu senden. Stellen Sie dabei sicher, daß die Nachricht für Ihren öffentlichen Schlüssel verschlüsselt wird.

Fehlermeldung	Ursache	Lösung
Die gekennzeichnete Eingabedatei ist nicht vorhanden.	Der eingegebene Dateiname existiert nicht.	Suchen Sie nach dem genauen Namen und Pfad der gewünschten Datei.
Es sind zur Zeit nicht genügend Zufallsdaten verfügbar.	Der Zufallsgenerator benötigt die Eingabe einer größeren Anzahl von Daten, um gültige willkürliche Zahlen zu erzeugen.	Wenn Sie dazu aufgefordert werden, bewegen Sie die Maus, oder drücken Sie willkürlich beliebige Tasten. Auf diese Weise werden Eingabedaten erzeugt.
Beim Erstellen eines Schlüsselbundes oder der exportierten Datei ist ein Fehler aufgetreten.	Daten konnten nicht in eine bestimmte Datei geschrieben werden.	Die Festplatte ist möglicherweise voll. Wenn sich die Datei auf einer Diskette befindet, befindet sich eventuell keine Diskette im Diskettenlaufwerk.
Beim Öffnen oder Erstellen des Schlüsselbundes oder der Ausgabedatei ist ein Fehler aufgetreten.	Eine benötigte Datei konnte nicht geöffnet werden.	Vergewissern Sie sich, daß die Einstellungen in den PGP-Voreinstellungen richtig sind. Wenn Sie kürzlich im PGP-Installationsverzeichnis Dateien gelöscht haben, müssen Sie möglicherweise das Produkt erneut installieren.
Dieser Schlüssel wurde bereits mit dem angegebenen Unterschriftenschlüssel unterschrieben.	Sie können einen Schlüssel nur einmal unterschreiben.	Sie haben versehentlich den falschen Schlüssel ausgewählt. Ist dies der Fall, wählen Sie einen anderen Schlüssel zum Unterschreiben aus.
Diese Datei ist schreibgeschützt oder in anderer Weise geschützt. Der Vorgang konnte daher nicht ausgeführt werden. Falls Sie Ihre Schlüsselbunddateien auf einem Wechseldatenträger speichern, ist möglicherweise das Volume nicht vorhanden.	Eine benötigte Datei ist schreibgeschützt oder wird von einem anderen Programm verwendet.	Schließen Sie andere Programme, die auf die gleichen Dateien wie das aktuelle Programm zugreifen. Wenn Sie Ihre Schlüsselbunddateien auf einer Diskette gespeichert haben, stellen Sie sicher, daß sich die Diskette im Diskettenlaufwerk befindet.

Problembehebung in PGPnet C

In diesem Anhang finden Sie Erläuterungen zu den Fehlermeldungen, die im PGPnet-Protokoll erscheinen können, Informationen zur Behebung von eventuell in PGPnet auftretenden Problemen sowie Angaben zu den PGPnet-Funktionen, mit denen Sie Probleme in PGPnet ausfindig machen und beseitigen können.

PGPnet-Fehlermeldungen

In der folgenden Tabelle haben wir die PGPnet-Fehlermeldungen, mögliche Ursachen und Vorschläge zur Behebung des Fehlers zusammengestellt.

Fehlermeldung	Ursache	Lösung
Ungültiger Austausch	Es wurde versucht, mit einer Phase 1-Vermittlung zu kommunizieren, die nicht mehr existiert. Phase 1 wurde zwar eingerichtet, eine Seite wurde jedoch heruntergefahren. Das kann auch passieren, wenn Sie eine SA löschen. Einige Produkte erkennen nicht, daß die SA beendet wurde, so daß weiterhin Informationen gesendet werden (das hat im allgemeinen keine negativen Folgen).	Richten Sie die SA neu ein.
Kein SPI gefunden	Ein Computer in der SA fällt aus, und der andere Computer erkennt das nicht. Die Fehlermeldung wird auf dem Computer angezeigt, der nicht erkennt, daß die SA ausgefallen ist.	Richten Sie die SA neu ein.
Keine SA gefunden	Höchstwahrscheinlich ein interner Fehler im PGP-Programm.	Informieren Sie NAI, wenn dieses Problem auftritt.
Ungültige Nutzinformationen	Wird üblicherweise durch Nichtübereinstimmung des gemeinsamen Geheimnisses verursacht. Kann auch durch beschädigte Netzwerkpakete verursacht werden (das Paket sagt, es sei 5 KB groß, obwohl es nur 4 KB groß ist).	Stellen Sie sicher, daß Sie dasselbe gemeinsame Geheimnis verwenden wie der andere Computer.

Fehlermeldung	Ursache	Lösung
Kein Vorschlag ausgewählt	Kann auftreten, wenn Computer A und Computer B verschiedene Konfigurationseinstellungen aufweisen.	Vergleichen Sie die Konfiguration des anderen Computers mit der Konfiguration Ihres eigenen Computers (Registerkarte **VPN - Erweitert** des Dialogfelds “Optionen”).
Ungültiges Cookie	Das Cookie ist zwischen Computer A und Computer B nicht mehr gültig. Ein Computer versucht, über eine SA zu kommunizieren, die beendet wurde. Ist im allgemeinen harmlos.	Richten Sie die SA neu ein.
Antwort-Timeout	1.) Routing-Problem. IP-Protokolle 50 und 51 UDP 500 für IKE. 2.) Sie senden Anfragen an einen Computer, der falsch konfiguriert ist.	Finden Sie heraus, ob es eine Firewall oder eine Einrichtung für die Übersetzung von Netzwerkadressen (Network Address Translation, NAT) gibt, die den Verbindungsaufbau verhindern.
NAT-Inkompatibilität wurde erkannt	Es gibt eine Einrichtung für die Übersetzung von Netzwerkadressen (Network Address Translation, NAT), die den Verbindungsaufbau verhindert.	Entfernen Sie die NAT-Einrichtung. NAT ist mit vielen Internet-Protokollen, darunter auch IPsec, nicht kompatibel.

Zusätzliche Tips

- Zur Fehlerbehebung können Sie das IKE-Protokoll verwenden. Das IKE-Protokoll öffnen Sie, indem Sie auf der Registerkarte **Protokoll** auf **Erweitert** klicken.
- Administratoren haben die Möglichkeit, die PGPnet-Konfigurationseinstellungen ihrer Benutzer zu “sperren”. Details hierzu finden Sie im *PGP-Administratorhandbuch*.
- Wenn die Kommunikation deutlich verlangsamt abläuft, sollten Sie die Komprimierungseinstellung auf der Registerkarte **VPN - Erweitert** überprüfen. Eventuell empfiehlt es sich, die Komprimierung auszuschalten. Beachten Sie, daß die Komprimierung nur bei DFÜ-Verbindungen sinnvoll ist.
- Wenn Sie auf einem Windows 98-Computer mehrere Netzwerkschnittstellen sichern, werden im Dialogfeld “Netzwerk” in der Systemsteuerung mehrere PGPnet-Adapter angezeigt.
- Treten beim Erstellen einer SA Probleme auf, verwenden Sie “SetAdapter” (**Start—>Programme—>PGP—>SetAdapter**), um sicherzustellen, daß die Kommunikation über die von Ihnen verwendete Netzwerkschnittstelle von PGPnet gesichert wird.
- Wenn Sie eine SA mit einem Rechner erstellen (in der SA-Spalte wird ein grünes Licht angezeigt) aber keinen Verkehr senden oder empfangen können, müssen Sie sicherstellen, daß PGPnet und die Netzwerkadressenübersetzung (NAT) die gleiche Einrichtung oder den gleichen Adapter verwenden.

  Es besteht möglicherweise eine Bindung zum falschen Adapter. Überprüfen Sie **SetAdapter** (**Start—>Programme—>PGP—>SetAdapter**).

Grundlagen der Authentisierung

Auf der Registerkarte **VPN-Authentisierung** wird festgelegt, wie Sie sich gegenüber anderen Rechnern authentisieren. Außerdem können Sie hier angeben, ob andere Rechner (konfigurierte oder nicht konfigurierte) eine gültige entfernte Authentisierung durchführen müssen, um mit Ihrem Rechner kommunizieren zu können.

Durch die Option **Entfernte Authentisierung** im Dialogfeld “Host/Gateway” wird bestimmt, wie sich ein bestimmter Host gegenüber Ihrem Rechner authentisiert.

Registerkarte “VPN-Authentisierung”

Mit Hilfe der Optionen **PGP-Authentisierung** und **X.509-Authentisierung** legen Sie fest, wie die Authentisierung Ihres lokalen Computers bei der Kommunikation mit anderen Computern erfolgen soll. Wenn Sie versuchen, eine SA zu erstellen, verwendet PGPnet den gewählten Schlüssel bzw. das gewählte Zertifikat, um dem anderen Computer mitzuteilen, wer Sie sind.

Legen Sie mit den Optionen in **Entfernte Authentisierung** fest, wie konfigurierte und unkonfigurierte Computer sich selbst authentisieren sollen.

Konfigurierte Hosts: Normalerweise werden Sie von konfigurierten Hosts einen gültigen Schlüssel oder ein Zertifikat zur Authentisierung anfordern. Klicken Sie dazu auf **Gültige entfernte Authentisierung von konfigurierten Hosts anfordern**. Wenn Sie wollen, daß ein konfigurierter Host einen bestimmten PGP-Schlüssel bzw. ein bestimmtes X.509-Zertifikat vorweisen muß, verwenden Sie die Option **Entfernte Authentisierung** im Dialogfeld “Host/Gateway”.

Nicht konfigurierte Hosts: Zwischen Ihnen und diesen Hosts hat möglicherweise noch keine Vertrauensbeziehung bestanden. Wenn ihnen der Verbindungsaufbau mit einem ungültigen Schlüssel bzw. einem ungültigen Zertifikat gestattet wird, wird der Verkehr verschlüsselt, während er sonst unverschlüsselt ablaufen würde.

- Um die Verbindung von unkonfigurierten Hosts mit einem Schlüssel bzw. einem Zertifikat zuzulassen, obwohl Ihr Schlüsselbund diesen bzw. dieses als nicht gültig betrachtet (der Schlüssel oder das Zertifikat kann aber durchaus gültig sein!), müssen Sie die Option **Gültige entfernte Authentisierung von nicht konfigurierten Hosts anfordern** deaktivieren.
- Wenn dagegen von unkonfigurierten Hosts eine gültige entfernte Authentisierung angefordert werden soll, aktivieren Sie die Option **Gültige entfernte Authentisierung von nicht konfigurierten Hosts anfordern**. Wenn diese Einstellung verwendet wird, wird eine Authentitätsprüfung des vom Server vorgelegten Schlüssels durchgeführt, und der Benutzer weist zu seiner eigenen Authentisierung sein anonymes Zertifikat vor. Das ist die Verfahrensweise, mit der auch die meisten E-Commerce-Websites arbeiten: Der Server wird authentisiert, der Client bleibt anonym.

Dialogfeld “Host/Gateway”: Entfernte Authentisierung

Mit den Optionen im Bereich **Entfernte Authentisierung** des Dialogfelds “Host / Gateway” können Sie den entfernten Host auffordern, jedesmal einen bestimmten PGP-Schlüssel oder ein bestimmtes X.509-Zertifikat vorzulegen, wenn er den Aufbau einer SA mit Ihrem Host versucht. Wenn der Host dann versucht, eine Verbindung aufzubauen und dabei nicht den festgelegten Schlüssel bzw. das festgelegte Zertifikat vorlegt, verweigert Ihr Rechner den Verbindungsaufbau.

Sie können diese Anforderung festlegen, wenn Sie im Expert-Modus einen Host hinzufügen. Für bereits bestehende Hosts läßt sich die Anforderung durch Bearbeitung des Hosteintrags hinzufügen.

HINWEIS: Die Hosts müssen ihren eigenen öffentlichen Schlüssel, nicht den öffentlichen Schlüssel von Ihnen, vorlegen.

WICHTIG: Wenn Sie für ein sicheres Teilnetz einen bestimmten PGP-Schlüssel oder ein bestimmtes X.509-Zertifikat wählen, müssen alle Benutzer in diesem Teilnetz den gleichen Schlüssel benutzen, um sich zu authentisieren. Das wäre jedoch eine ungewöhnliche Konfiguration.

Alle Schlüsselauthentisierungen werden auf der Registerkarte **Protokoll** angezeigt, und für jeden Eintrag wird die Schlüssel-ID angegeben.

Von der PGPnet-Funktion IDS erkannte häufig vorkommende Angriffe

D

In der folgenden Tabelle werden die Angriffe aufgeführt, die von der PGPnet-Funktion IDS (Angrifferkennungssystem) erkannt werden können. Die einzelnen Angriffe werden beschrieben, und es wird für jeden Angriff der Risikofaktor angegeben.

Angriff	Beschreibung	Risikofaktor
Back Orifice	Back Orifice ist ein Backdoor-Programm für Windows 9x, das von der Hackergruppe “Cult of the Dead Cow” geschrieben wurde. Sobald dieses Backdoor-Programm installiert ist, können auf dem jeweiligen Rechner über Fernzugriff unter anderem Befehle ausgeführt, Screenshots erfaßt, die Registrierung geändert sowie andere Operationen ausgeführt werden. Client-Programme zum Zugriff auf Back Orifice sind für Windows und UNIX verfügbar.	Hoch
Bonk	Dieser Angriff nutzt einen Implementierungsfehler in Microsofts erstem Teardrop-Patch und kann als Windows-spezifische Variante des ursprünglichen Teardrop-Angriffs angesehen werden.	Hoch
Fraggle	Dieser Angriff ist eine UDP-Variante des Smurf-Angriffs. Durch das Versenden eines gefälschten UDP-Pakets an einen bestimmten Port einer Broadcast-Adresse antworten die Systeme im “Verstärker”-Netzwerk dem Zielrechner mit einer UDP-Antwort oder mit einem ICMP UNREACHABLE-Paket. Diese Flut eingehender Pakete führt zu einem “Denial-of-Service”-Angriff gegen den Zielrechner.	Hoch
IP Spoofing	Beim IP Spoofing werden Daten mit einer gefälschten IP-Adresse für Rückantworten gesendet. An sich stellt dieses Spoofing einer IP-Quelladresse keine Gefahr dar; diese Technik kann aber zusammen mit anderen Verfahren verwendet werden, um Angriffe (Hijacking von TCP-Sitzungen) auszuführen oder um die Quelle von “Denial-of-Service”-Angriffen (SYN-Flood, PING-Flood usw.) zu verschleiern.	Mittel

Angriff	Beschreibung	Risikofaktor
Jolt	Remote-“Denial-of-Service”-Angriff, bei dem spezielle ICMP-Paketfragmente verwendet werden. Er kann die Zielsysteme verlangsamen oder zum Absturz bringen.	Hoch
Jolt2	Jolt ähnlicher Remote-“Denial-of-Service”-Angriff, bei dem spezielle ICMP- oder UDP-Paketfragmente verwendet werden. Er kann die Zielsysteme verlangsamen oder zum Absturz bringen.	Hoch
Land	Bei diesem Angriff wird ein TCP-Paket zu einem laufenden Service auf einem Zielhost gesendet, wobei eine Quelladresse desselben Hosts verwendet wird. Beim TCP-Paket handelt es sich um ein SYN-Paket, das zum Herstellen einer neuen Verbindung genutzt wird. Der TCP-Quellport ist dabei mit dem Zielport identisch. Wenn der Zielhost dieses Paket akzeptiert, verursacht es eine Schleife innerhalb des Betriebssystems, wodurch sich das System “aufhängt”.	Hoch
Nestea	Dieser Angriff nutzt einen Fehler bei der Berechnung der Größen bei der Paketfragment-Reassemblierung. In der Reassemblierungsroutine ungeschützter Systeme konnte die Länge des IP-Header-Felds nicht ermittelt werden. Deshalb kann es durch das Senden gezielt zusammengestellter Pakete an ein ungeschütztes System zum Zusammenbruch des Zielsystems kommen.	Hoch
Ping Flood	Bei diesem Angriff werden Unmengen von ICMP ECHO (PING)-Anfragen an den angegriffenen Host gesendet. Diese Art des Angriffs ist besonders wirkungsvoll, wenn der Angreifer über eine schnellere Netzwerkverbindung verfügt als der Angegriffene.	Hoch
Ping of Death	Bei diesem Angriff kann Ihr System durch Fernzugriff destabilisiert oder neugestartet werden, indem ein überdimensioniertes PING-Paket an das System gesendet wird. Das geschieht durch Senden eines fragmentierten Pakets mit einer Länge über 65536 Bytes, wodurch das Remote-System das System nicht richtig verarbeiten kann. Das Remote-System reagiert darauf mit einem Neustart oder meldet eine Systemüberlastung.	Hoch

Angriff	Beschreibung	Risikofaktor
Port Scanning	Das Port Scanning selbst stellt zwar noch keinen Angriff dar, aber es deutet oft darauf hin, daß ein Angreifer Ihr System bereits auf mögliche Schwachstellen untersucht hat. Beim Port Scanning werden alle TCP- oder/und UDP-Ports auf vorhandene Services (und damit auf potentielle Angriffspunkte) überprüft.	Niedrig
Smurf	Bei diesem Angriff wird ein ICMP ECHO REQUEST (PING)-Paket mit einer gefälschten Quelladresse gesendet, die der Adresse des Zielsystems entspricht. Dieses Paket wird an sogenannte “Verstärker”-Netzwerke gesendet (Netzwerke, die das Senden von Paketen an die Broadcast-Adresse gestatten), so daß sämtliche Rechner im Verstärkernetzwerk auf diese angeblich berechtigte Anforderung vom Ziel antworten. Das führt dazu, daß das Zielsystem mit ICMP ECHO REPLY-Meldungen überflutet wird, so daß ein “Denial-of-Service”-Angriff entsteht.	Hoch
SYN Flood	Mit diesem Angriff können Netzwerkdienste völlig zum Erliegen gebracht werden, indem sie mit Verbindungsanforderungen überflutet werden. Dadurch wird die Warteschlange mit der Liste der noch nicht hergestellten eingehenden Verbindungen völlig aufgefüllt, so daß keine weiteren Verbindungsanforderungen mehr angenommen werden.	Hoch
Teardrop	Bei ungeschützten Systemen kann ein Fehler ausgenutzt werden, den der TCP/IP-Stapelspeicher bei der Behandlung fragmentierter Paket-Reassemblierungen aufweist. Dadurch werden verfügbare Speicherressourcen in Anspruch genommen. Durch das Senden eines speziell zugeschnittenen IP-Datagramms kann dieser Angriff bei vielen Betriebssystemen zum “Aufhängen” führen oder einen Neustart bewirken.	Hoch
UDP Flood	Remote-“Denial-of-Service”-Angriff, bei dem der Zielrechner mit weitaus mehr Daten überflutet wird, als er verarbeiten kann, wodurch legitime Verbindungen nicht mehr hergestellt werden können.	Hoch

Liste biometrischer Worte

Von Philip Zimmermann und Patrick Juola

Die authentisierte Übertragung binärer Informationen erfolgt in PGP anhand einer speziellen Wortliste über einen Sprechkanal, beispielsweise ein Telefon, und zwar unter Verwendung biometrischer Unterschriften. Vorausgesetzt, der jeweilige Zuhörer versteht sie, dienen die durch die menschliche Stimme gesprochenen Worte der biometrischen Authentisierung der Daten, die in gesprochener Form übermittelt werden. Die Wortliste hat denselben Zweck wie das Militäralphabet, das zur Übertragung von Buchstaben über einen verrauschten Funksprechkanal verwendet wird. Das Militäralphabet umfaßt jedoch 26 Worte, wobei jedes Wort für einen Buchstaben steht. Für unsere Zwecke enthält unsere Liste 256 sorgfältig ausgewählte, phonetisch eindeutige Worte, die für die 256 möglichen Byte-Werte von 0 bis 255 stehen.

Wir haben eine Wortliste ausgearbeitet, anhand derer binäre Informationen per Telefon übermittelt werden können; jedes Wort steht hierbei für einen anderen Byte-Wert. Dabei waren wir bemüht, die Liste so zu gestalten, daß sie mit einer Vielzahl von Anwendungen einsetzbar ist. Die erste dieser Anwendungen sollte die Fingerabdrücke des öffentlichen Schlüssels aus PGP über das Telefon lesen, um den öffentlichen Schlüssel so zu authentisieren. In diesem Fall ist der Fingerabdruck 20 Byte lang – es müssen also 20 Worte laut vorgelesen werden. Aus Erfahrung wissen wir, daß das Lesen so vieler Byte in Hexadezimalform relativ aufwendig und fehleranfällig ist. Die Verwendung einer Wortliste, in der jedes Byte durch ein Wort dargestellt wird, scheint sich in diesem Fall also anzubieten.

Bei einigen Anwendungen ist es möglicherweise sogar erforderlich, noch deutlich längere Byte-Folgen per Telefon zu übertragen; dies trifft beispielsweise auf vollständige Schlüssel oder Unterschriften zu. Hierbei müssen unter Umständen über 100 Byte gelesen werden. In diesem Fall scheint es oft sinnvoller zu sein, Worte anstelle von Hexadezimalbyte zu verwenden.

Beim lauten Vorlesen langer Byte-Folgen schleichen sich leicht Fehler ein. Die Art Fehler, die bei der Sprachübertragung von Daten auftreten, unterscheiden sich von den Fehlern, die bei der Datenübertragung per Modem vorkommen. Bei Modems werden Bit normalerweise durch Leitungsgeräusche gestört. Zur Fehlererkennung werden bei Modems meist CRCs hinzugefügt, die optimiert wurden, um Signalbündel von Leitungsgeräuschen zu erkennen. Bei willkürlichen Folgen gesprochener Worte kommt es üblicherweise zu einem der folgenden drei Fehler: 1) Vertauschung zweier aufeinanderfolgender Worte, 2)

doppelte Worte oder 3) ausgelassene Worte. Bei der Entwicklung einer Fehlererkennungsmethode für diese Art von Datenübertragungskanal sollte besonderes Augenmerk auf der Abstimmung auf diese drei Fehlerarten liegen. 1991 unterhielt ich mich mit Zhahai Stewart, der eine gute Methode zur Fehlererkennung bezüglich dieser Fehler vorzuschlagen hatte.

Stewarts Ansatz zur Fehlererkennung beim lauten Vorlesen langer Byte-Folgen unter Verwendung einer Wortliste sieht vor, nicht nur eine, sondern zwei solcher Listen zu verwenden. Jede Liste enthält 256 phonetisch eindeutige Worte; jedes Wort steht für einen anderen Byte-Wert zwischen 0 und 255.

Das erste Byte (Versatz 0 in der Folge) wird zur Auswahl eines Wortes in der Liste mit den geraden Einträgen verwendet. Das Byte bei Versatz 1 wird zur Auswahl eines Wortes in der Liste mit den ungeraden Einträgen verwendet. Das Byte bei Versatz 2 wählt wieder ein Wort in der Liste der geraden Einträge, und das Byte bei Versatz 3 trifft wieder eine Auswahl in der Liste der ungeraden Einträge. Tatsächlich wird jeder Byte-Wert durch zwei unterschiedliche Worte dargestellt, abhängig davon, ob das jeweilige Byte vom Beginn der Byte-Folge gesehen bei einem geraden oder ungeraden Versatz angezeigt wird. Nehmen wir beispielsweise an, daß sowohl das Wort “adult” als auch das Wort “amulet” in den beiden Wortlisten jeweils an derselben Position aufgeführt wird, nämlich an Position 5. Das bedeutet, daß die wiederholende 3-Byte-Folge 05 05 05 für die 3-Wort-Folge “adult, amulet, adult” steht.

Bei dieser Vorgehensweise lassen sich alle drei gängigen Fehlerarten in Sprachdatenströmen problemlos erkennen: Vertauschung, Duplikation und Auslassung. Bei einer Vertauschung werden zwei aufeinanderfolgenden Worten aus der Liste mit geraden Einträgen zwei aufeinanderfolgende Worte aus der Liste mit ungeraden Einträgen nachgestellt (oder andersherum). Eine Duplikation fällt durch zwei aufeinanderfolgende doppelte Worte auf, etwas, was in einer normalen Folge nicht vorkommt. Bei einer Auslassung werden zwei aufeinanderfolgende Worte aus derselben Liste verwendet.

Um die sofortige und zweifelsfreie Entdeckung der oben erläuterten drei Fehlerarten ohne Computerunterstützung zu ermöglichen, haben wir zwei Listen erarbeitet, die sich in einem Punkt deutlich unterscheiden: In der Liste mit den geraden Einträgen sind ausschließlich zweisilbige Worte, in der Liste mit den ungeraden Einträgen sind hingegen ausschließlich dreisilbige Worte enthalten. Dieser Vorschlag wurde von Computerlinguist Patrick Juola unterbreitet.

Die tatsächliche Ausarbeitung der Wortliste durch Patrick Juola und Phil Zimmermann wurde durch die Anwendung PGPfone beschleunigt. PGPfone ist eine Anwendung, durch die Ihr Computer zu einem sicheren Telefon wird. Wir haben diese Anwendung zur Authentisierung des erstmaligen Diffie-Hellman-Schlüsselaustauschs verwendet; digitale Unterschriften und Infrastrukturen öffentlicher Schlüssel kamen hierbei nicht zum Einsatz. Wir wußten, daß wir sie bei der Anwendung auf PGP zu einem späteren Zeitpunkt zur Authentisierung von Fingerabdrücken von PGP-Schlüsseln erneut verwenden würden.

Durch die Ausarbeitung der Wortlisten wollten wir eine Einheit zum Messen des phonetischen Abstands zwischen zwei Worten entwickeln, die dann als Anhaltspunkt zur Ausarbeitung einer vollständigen Liste dienen sollte. Grady Ward stellte uns eine umfangreiche Zusammenstellung von Worten und deren Aussprache zur Verfügung, und Patrick Juola erstellte mit genetischen Algorithmen die am besten geeignete Teilmenge aus Grady Wards Liste. Hier eine kurze Zusammenfassung von Juolas Arbeit: Er stellte eine große Anzahl von Annahmen auf, die er sich “vermehren” ließ (durch den Ersatz von Annahmen durch andere Worte). Wie in der Entwicklungsgeschichte bildeten die besser geeigneten Annahmen die nächste Generation. Nach etwa 200 Generationen war die Liste ihrer Idealform schon sehr nahegekommen: Der phonetische Abstand zwischen den Worten war deutlich größer als bei der ursprünglichen Liste.

Die erste große Hürde war die Entwicklung der Metrik. Linguisten befassen sich seit Jahrzehnten mit der Erzeugung und Wahrnehmung von Tönen, und es gibt eine Reihe von Standardausdrücken, mit denen die Töne in der jeweiligen Sprache beschrieben werden. Wenn Sie zum Beispiel die englischen Worte “pun”, “fun”, “dun” und “gun” sagen (versuchen Sie es ruhig einmal), fällt auf, daß sich die Zunge bei jedem dieser Worte nach hinten bewegt. Linguisten bezeichnen dies als “Artikulationspunkt”. Geräusche, die sich diesbezüglich deutlich unterscheiden, hören sich für englische Muttersprachler unterschiedlich an. Wenn die Merkmale aller Töne in einem Wort kombiniert werden, erhalten wir die Tondarstellung des gesamten Wortes – und wir können den phonetischen Abstand zwischen einem Wortpaar errechnen.

Ganz so einfach war es dann doch nicht. Wir wußten nicht, welche Bedeutung den einzelnen Merkmalen zukommt, wortebenenbezogene Merkmale wie Akzente ließen sich nur schwer darstellen, und für bestimmte Töne war die merkmalsbasierte Analyse schlichtweg nicht durchführbar. Außerdem gab es noch einige weitere Feinheiten: Wir suchten nach Worten, die gängig genug waren, um allgemein bekannt zu sein – sie sollten jedoch wiederum nicht langweilig sein. Verwirrende Worte wie “Wiederholen”, “Anfangen” oder “Fehler” sollten vermieden werden. Personen, deren Muttersprache nicht Englisch ist, nehmen bestimmte Tonmerkmale weniger ausgeprägt war. Ein Beispiel: Für Personen mit japanischer Muttersprache hören sich “r” und “l” möglicherweise gleich an und werden folglich auch gleich ausgesprochen. Wenn die

Worte so kurz wären, daß eine ausreichende Anzahl davon auf einem kleinen LCD-Display Platz findet, wäre dies ebenfalls von Vorteil. Große Konsonantenblöcke (“corkscrew” enthält fünf betonte Konsonanten hintereinander) sind in einigen Fällen schwer auszusprechen, besonders für Personen, deren Muttersprache nicht Englisch ist. Wie dem auch sei, wir waren bemüht, anhand all dieser Kriterien einen Filter für die ursprüngliche Wörterbuchliste bzw. für die Abstandsmetrik selbst zu erstellen.

Nachdem der Computer die am besten geeignete Liste “ausgespuckt” hatte, sahen wir sie uns noch einmal genau an. Ja, die Worte waren phonetisch eindeutig. Viele sahen jedoch so aus, als wären sie von einem Computer, nicht von einem menschlichen Wesen, ausgewählt worden. Eine Menge der Worte waren schlichtweg schrecklich und dumm. Einige waren abstoßend, andere waren nichtssagend und fad. Also haben wir die Liste ein bißchen “aufgefrischt”. Einige Worte wurden gelöscht und durch solche ersetzt, die ein menschliches Wesen ausgesucht hätte. Wir ließen den Computer die neuen Worte mit der Liste vergleichen, um deren phonetische Eindeutigkeit im Vergleich zur restlichen Liste sicherzustellen. Außerdem versuchten wir, die Worte so zu gestalten, daß es nicht zu phonetischen Konflikten mit den anderen Worten im größeren Wörterbuch kommen konnte. Hierzu mußten wir darauf achten, daß die ausgewählten Worte nicht versehentlich für andere gehalten wurden, die sich nicht auf der Liste befanden.

In seinen Algorithmen verwendete Patrick Juola eine Reihe von Auswahlkriterien. Zu diesem Thema veröffentlichte er ein Dokument, in dem die Vorgänge detaillierter beschrieben werden. Das vorliegende Dokument bietet lediglich einen kurzen Abriß unserer Vorgehensweise bei der Ausarbeitung der Liste.

Ich bin mit der Wortliste nicht hundertprozentig zufrieden. Wenn es nach mir ginge, sollten mehr eingängige und weniger nichtssagende Worte enthalten sein. Mir persönlich gefallen Worte wie “Aztec” und “Capricorn” und die Worte im standardmäßigen Militäralphabet. Obwohl wir uns das Recht vorbehalten möchten, die Liste zu einem späteren Zeitpunkt zu überarbeiten, ist dies aufgrund der Probleme, die durch diese erste Version entstehen werden, eher unwahrscheinlich. Die vorliegende Version der Liste wurde zuletzt im September 1998 geändert.

Wortliste mit zweisilbigen Einträgen

aardvark	absurd	accrue	acme	adrift
adult	afflict	ahead	aimless	Algol
allow	alone	ammo	ancient	apple
artist	assume	Athens	atlas	Aztec
baboon	backfield	backward	banjo	beaming
bedlamp	beehive	beeswax	befriend	Belfast
berserk	billiard	bison	blackjack	blockade
blowtorch	bluebird	bombast	bookshelf	brackish
breadline	breakup	brickyard	briefcase	Burbank
button	buzzard	cement	chairlift	chatter
checkup	chisel	choking	chopper	Christmas
clamshell	classic	classroom	cleanup	clockwork
cobra	commence	concert	cowbell	crackdown
cranky	crowfoot	crucial	crumpled	crusade
cubic	dashboard	deadbolt	deckhand	dogsled
dragnet	drainage	dreadful	drifter	dropper
drumbeat	drunken	Dupont	dwelling	eating
edict	egghead	eightball	endorse	endow
enlist	erase	escape	exceed	eyeglass
eyetooth	facial	fallout	flagpole	flatfoot
flytrap	fracture	framework	freedom	frighten
gazelle	Geiger	glitter	glucose	goggles
goldfish	gremlin	guidance	hamlet	highchair
hockey	indoors	indulge	inverse	involve
island	jawbone	keyboard	kickoff	kiwi
klaxon	locale	lockup	merit	minnow
miser	Mohawk	mural	music	necklace
Neptune	newborn	nightbird	Oakland	obtuse
offload	optic	orca	payday	peachy
pheasant	physique	playhouse	Pluto	preclude
prefer	preshrunk	printer	prowler	pupil
puppy	python	quadrant	quiver	quota
ragtime	ratchet	rebirth	reform	regain
reindeer	rematch	repay	retouch	revenge
reward	rhythm	ribcage	ringbolt	robust
rocker	ruffled	sailboat	sawdust	scallion
scenic	scorecard	Scotland	seabird	select
sentence	shadow	shamrock	showgirl	skullcap
skydive	slingshot	slowdown	snapline	snapshot
snowcap	snowslide	solo	southward	soybean
spaniel	spearhead	spellbind	spheroid	spigot
spindle	spyglass	stagehand	stagnate	stairway
standard	stapler	steamship	sterling	stockman
stopwatch	stormy	sugar	surmount	suspense
sweatband	swelter	tactics	talon	tapeworm
tempest	tiger	tissue	tonic	topmost
tracker	transit	trauma	treadmill	Trojan
trouble	tumor	tunnel	tycoon	uncut
unearth	unwind	uproot	upset	upshot
vapor	village	virus	Vulcan	waffle
wallet	watchword	wayside	willow	woodlark
Zulu				

Wortliste mit dreisilbigen Einträgen

adroitness	adviser	aftermath	aggregate	alkali
almighty	amulet	amusement	antenna	applicant
Apollo	armistice	article	asteroid	Atlantic
atmosphere	autopsy	Babylon	backwater	barbecue
belowground	bifocals	bodyguard	bookseller	borderline
bottomless	Bradbury	bravado	Brazilian	breakaway
Burlington	businessman	butterfat	Camelot	candidate
cannonball	Capricorn	caravan	caretaker	celebrate
cellulose	certify	chambermaid	Cherokee	Chicago
clergyman	coherence	combustion	commando	company
component	concurrent	confidence	conformist	congregate
consensus	consulting	corporate	corrosion	councilman
crossover	crucifix	cumbersome	customer	Dakota
decadence	December	decimal	designing	detector
detergent	determine	dictator	dinosaur	direction
disable	disbelief	disruptive	distortion	document
embezzle	enchanting	enrollment	enterprise	equation
equipment	escapade	Eskimo	everyday	examine
existence	exodus	fascinate	filament	finicky
forever	fortitude	frequency	gadgetry	Galveston
getaway	glossary	gossamer	graduate	gravity
guitarist	hamburger	Hamilton	handiwork	hazardous
headwaters	hemisphere	hesitate	hideaway	holiness
hurricane	hydraulic	impartial	impetus	inception
indigo	inertia	infancy	inferno	informant
insincere	insurgent	integrate	intention	inventive
Istanbul	Jamaica	Jupiter	leprosy	letterhead
liberty	maritime	matchmaker	maverick	Medusa
megaton	microscope	microwave	midsummer	millionaire
miracle	misnomer	molasses	molecule	Montana
monument	mosquito	narrative	nebula	newsletter
Norwegian	October	Ohio	onlooker	opulent
Orlando	outfielder	Pacific	pandemic	Pandora
paperweight	paragon	paragraph	paramount	passenger
pedigree	Pegasus	penetrate	perceptive	performance
pharmacy	phonetic	photograph	pioneer	pocketful
politeness	positive	potato	processor	provincial
proximate	puberty	publisher	pyramid	quantity
racketeer	rebellion	recipe	recover	repellent
replica	reproduce	resistor	responsive	retraction
retrieval	retrospect	revenue	revival	revolver
sandalwood	sardonic	Saturday	savagery	scavenger
sensation	sociable	souvenir	specialist	speculate
stethoscope	stupendous	supportive	surrender	suspicious
sympathy	tambourine	telephone	therapist	tobacco
tolerance	tomorrow	torpedo	tradition	travesty
trombonist	truncated	typewriter	ultimate	undaunted
underfoot	unicorn	unify	universe	unravel
upcoming	vacancy	vagabond	vertigo	Virginia
visitor	vocalist	voyager	warranty	Waterloo
whimsical	Wichita	Wilmington	Wyoming	yesteryear
Yucatan				

Produkt-Support F

Kontakt mit McAfee

BEVOR Sie sich mit dem Technischen Support von McAfee Software in Verbindung setzen, stellen Sie bitte Zugriff auf den Rechner, auf dem PGP installiert ist sicher und halten folgende Informationen bereit:

- Haben Sie die Registrierungskarte eingeschickt?
- PGP-Version
- Wie lautet Ihre Kundennummer (falls registriert)?
- Mit welchem Festplattenmodell arbeiten Sie (intern oder extern)?
- Mit welcher System-Software arbeiten Sie?
- Wie groß ist Ihr Arbeitsspeicher (RAM)?
- Welche zusätzlichen Karten, Platinen oder Monitore sind installiert?
- Wie lauten Name und Version der Software, bei der das Problem auftritt?
- Welche Fehlermeldung (WORTLAUT!) wird auf dem Bildschirm angezeigt?
- Welche Schritte haben Sie unmittelbar vor Auftreten der Fehlermeldung ausgeführt?
- Beschreiben Sie das Problem möglichst vollständig:

Customer Service

Um Produkte zu bestellen oder Produktinformationen zu erhalten, wenden Sie sich an den McAfee Customer Service unter 0800-1005262, oder schreiben Sie an die folgende Adresse:

McAfee
Gatwickstraat 25
1043 GL Amsterdam
Niederlande

E-Mail: **single_user_europe@nai.com**

Technischer Support

Support über das Web

Network Associates ist bekannt für sein Engagement in Sachen Kundenzufriedenheit. Wir setzen diese Tradition fort, indem wir unsere Site im World Wide Web (http://www.mcafee-at-home.de) zu einer wertvollen Ressource für Fragen an den technischen Support gemacht haben.

Wir empfehlen Ihnen, sie zu Ihrer ersten Quelle für Antworten auf häufig gestellte Fragen, Updates von McAfee-Software und den Zugriff auf McAfee-News und -Virusinformationen zu machen.

Die Informationen im McAfee KnowledgeCenter stehen Ihnen Tag und Nacht an sieben Tage die Woche zur Verfügung (http://www.mcafee.de/jump_nai.asp?url=http://www.support.mcafee.com/tech_supp/pkc.asp)

Support-Foren und telefonische Kontaktaufnahme

Wenn Sie das Gesuchte nicht finden oder keinen Webzugriff haben, probieren Sie einen unserer automatischen Dienste aus.

Tabelle F-1 .

World Wide Web	www.mcafee-at-home.de
CompuServe	GO MCAFEE
America Online (AOL)	Kennwort MCAFEE
Microsoft Network	mcafee

Glossar

AES (Advanced Encryption Standard)	Vom National Institute of Standards and Technology (NIST) anerkannter Verschlüsselungsstandard, der in der Regel in den nächsten 20 bis 30 Jahren gültig sein wird.
AH (Authentication Header)	Sicherheitsprotokoll für die Authentisierung. AH wird in die zu schützenden Daten eingebettet. Es kann entweder allein oder zusammen mit ESP (Encryption Service Payload) verwendet werden.
Algorithmus (Hash)	Gruppe von mathematischen (logischen) Regeln, die für die Erstellung von Nachrichtenkernen und die Erzeugung von Schlüsseln/Unterschriften verwendet werden.
Algorithmus (Verschlüsselung)	Gruppe von mathematischen (logischen) Regeln, die für die Verschlüsselung und Entschlüsselung verwendet werden.
Anonymität	Ursprung oder Autor der Informationen ist unbekannt oder nicht angegeben, so daß die Identität des Erstellers/Absenders nicht herausgefunden werden kann.
ANSI (American National Standards Institute)	Entwickelt Standards über verschiedene akkreditierte Normen-Gremien (Accredited Standards Committee; ASC). Das X9-Komitee beschäftigt sich vorwiegend mit Sicherheitsstandards für Finanzdienstleistungen.
ASCII-Text	Binäre Informationen, die in druckbarem ASCII-Standardzeichensatz mit 7 Bit verschlüsselt wurden. Dies dient der einfacheren Übertragung über Kommunikationssysteme. Bei PGP werden ASCII-geschützte Textdateien mit ihrer standardmäßigen Dateinamenerweiterung versehen. Sie werden im ASCII-Format (Basis 64) ver- und entschlüsselt.
Asymmetrische Schlüssel	Ein zwar separates, jedoch integriertes Benutzerschlüsselpaar, bestehend aus einem öffentlichen und einem privaten Schlüssel. Es handelt sich dabei um Einwegschlüssel, d. h. ein Schlüssel, der zur Verschlüsselung bestimmter Daten verwendet wurde, kann nicht zur Entschlüsselung derselben Daten benutzt werden.
Authentisierung	Die Ermittlung des Ursprungs verschlüsselter Informationen durch die Überprüfung der digitalen Unterschrift oder des öffentlichen Schlüssels einer Person, indem der eindeutige Fingerabdruck überprüft wird.

Automatische Schlüsselerneuerung

Für die Erstellung Ihrer Sicherheitsverbindungen (Security Associations, SAs) werden die Einrichtungsschlüssel (IKE) und die Primärschlüssel (IPsec) herangezogen. Diese werden auf der Grundlage der auf der Registerkarte “VPN” in den PGP-Optionen festgelegten Werte für “Automatische Schlüsselerneuerung”(Windows) bzw. “VPN-Aktualisierung” (Mac) automatisch erneuert.

Autorisierter Schlüsselverwalter

Eine Person, der Sie dahingehend vertrauen, daß sie Ihnen echte Schlüssel anbietet. Wenn ein autorisierter Schlüsselverwalter einen fremden Schlüssel unterzeichnet, müssen Sie die Gültigkeit dieses Schlüssels nicht mehr in Frage stellen.

Back Orifice

Back Orifice ist ein Backdoor-Programm für Windows 9x, das von der Hackergruppe “Cult of the Dead Cow” geschrieben wurde. Sobald dieses Backdoor-Programm installiert ist, können auf dem jeweiligen Rechner über Fernzugriff unter anderem Befehle ausgeführt, Screenshots erfaßt, die Registrierung geändert sowie andere Operationen ausgeführt werden. Client-Programme zum Zugriff auf Back Orifice sind für Windows und UNIX verfügbar.

Backdoor

Beabsichtigter oder unbeabsichtigter Fehler im Chiffrierungsverfahren, durch den die angebliche Stärke der Verschlüsselung mittels eines Tricks problemlos ausgehebelt werden kann. Wenn der Entwicklungshintergrund des Chiffrierungsverfahrens geheim gehalten wird, wird häufig das Vorhandensein einer solchen “Hintertür” (Backdoor) vermutet.

Benutzer-ID

Eine Textphrase, mit der ein Schlüsselpaar identifiziert wird. Ein übliches Format für eine Benutzer-ID ist beispielsweise der Name und die E-Mail-Adresse des Eigentümers. Mit der Benutzer-ID können Benutzer (d. h. sowohl der Eigentümer selbst als auch dessen Kollegen) den Eigentümer des Schlüsselpaars erkennen.

Blinde Unterschrift

Möglichkeit zum Unterschreiben von Dokumenten ohne Kenntnis des Inhalts, ähnlich wie bei zur Beglaubigung von Dokumenten berechtigten öffentlichen Stellen.

Blockverschlüsselung

Ein symmetrischer Chiffriercode, der auf der Basis von Blöcken (in der Regel 64-Bit-Blöcke) von Klartext und verschlüsseltem Text funktioniert.

CA (Certificate Authority)

Ein vertrauenswürdiger Dritter (Trust Third- Party; TTP), der Zertifikate mit Beurteilungen über verschiedene Attribute erstellt und diese einem Benutzer und/oder dem zugehörigen öffentlichen Schlüssel zuordnet.

CAPI (Crypto API)

Die Kryptographie-API von Microsoft für Windows-basierte Betriebssysteme und Anwendungen.

CAST

Ein 64-Bit-Blockchiffrierer, der 64-Bit-Schlüssel, sechs S-Boxen mit 8-Bit-Eingabe und 32-Bit-Ausgabe verwendet. Er wurde in Kanada von Carlisle Adams und Stafford Tavares entwickelt.

Chiffrierter Text	Klartext, der mit einem Verschlüsselungsalgorithmus in ein nicht lesbares Format verarbeitet wurde. Mit einem Entschlüsselungsschlüssel kann dieser Vorgang rückgängig gemacht und der Originaltext wieder hergestellt werden.
CRYPTOKI	Entspricht PKCS #11.
Datenintegrität	Ein Verfahren zum Prüfen, ob Informationen noch im Ursprungszustand vorliegen und nicht durch Unbefugte oder auf unbekannte Weise verändert wurden.
Denial-of-Service-Angriff	Üblicherweise geplanter Angriff mit dem Ziel, die Verfügbarkeit des Servers im Internet zu unterbrechen. Bei einem “Denial-of-Service”-Angriff wird ein Internet-Server mit Verbindungsanforderungen überschwemmt, die nicht ausgeführt werden können. Der Server versucht, auf die Anforderungen zu antworten und wird dabei so ausgelastet, daß er legitime Verbindungsanforderungen ignoriert.
DES (Data Encryption Standard)	Eine 64-Bit-Blockchiffrierung oder ein symmetrischer Algorithmus, der auch als Data Encryption Algorithm (DEA) (vom ANSI) bzw. DEA-1 (von der ISO) bezeichnet wird. Seit über 20 Jahren weit verbreitet, 1976 übernommen als “FIPS 46”.
Diffie-Hellman	Der erste Verschlüsselungsalgorithmus für öffentliche Schlüssel, der diskrete Logarithmen in einem endlichen Feld verwendete. Er wurde 1976 erfunden.
Digitale Unterschrift	Siehe “Unterschrift”.
Digitalgeld	Geld in elektronischer Form, das über eine Vielzahl von komplexen Protokollen gespeichert und übertragen wird.
Direktes Vertrauen	Schaffung von Vertrauen auf gegenseitiger Basis.
DSA (Digital Signature Algorithm)	Ein vom NIST entworfener digitaler Unterschriftenalgorithmus für öffentliche Schlüssel zur Verwendung in DSS.
DSS (Digital Signature Standard)	Ein vom NIST vorgeschlagener Standard (FIPS) für digitale Unterschriften unter Verwendung des DSA.
ECC (Elliptic Curve Cryptosystem)	Ein eindeutiges Verfahren zur Erstellung von Verschlüsselungsalgorithmen für öffentliche Schlüssel auf der Grundlage von mathematischen Kurven in endlichen Feldern oder mit großen Primzahlen.
EES (Escrowed Encryption Standard)	Ein von der amerikanischen Regierung vorgeschlagener Standard zur Hinterlegung privater Schlüssel.
Einrichtungsschlüssel (IKE)	IKE-Schlüssel für das Erstellen Ihrer Sicherheitsverbindungen. Werte können als zeitliche Werte festgelegt werden.

Einweg-Hash
Eine Funktion einer variablen Zeichenfolge zum Erstellen eines Wertes mit fester Länge, der das ursprüngliche Abbild darstellt. Wird auch Nachrichtenkern, Fingerabdruck und Message Integrity Check (MIC) genannt.

Elgamal-Schema
Wird für digitale Unterschriften und zur Verschlüsselung auf der Basis von diskreten Logarithmen in einem endlichen Feld verwendet. Kann mit der DAS-Funktion kombiniert werden.

Entschlüsselung
Eine Methode, mit der die Verschlüsselung von Informationen rückgängig gemacht werden kann, so daß diese wieder lesbar werden. Die Entschlüsselung wird mit dem privaten Schlüssel des Empfängers durchgeführt.

ESP (Encapsulating Security Payload)
IPsec-Header, der den Inhalt von IP-Paketen verschlüsselt.

Fingerabdruck
Eine eindeutig identifizierende Zahlen- und Zeichenfolge zur Authentisierung öffentlicher Schlüssel. Dies ist das Hauptkriterium für die Überprüfung der Echtheit eines Schlüssels. Siehe *Fingerabdruck des Schlüssels*.

Fingerabdruck eines Schlüssels
Eine eindeutig identifizierende Zahlen- und Zeichenfolge zur Authentisierung öffentlicher Schlüssel. Sie können beispielsweise den Eigentümer eines öffentlichen Schlüssels anrufen und sich nach dem Fingerabdruck seines Schlüssels erkundigen, um diesen mit Ihrem Fingerabdruck des öffentlichen Schlüssels zu vergleichen und zu sehen, ob beide Schlüssel miteinander übereinstimmen. Falls die Fingerabdrücke nicht übereinstimmen, ist einer der Schlüssel falsch.

FIPS (Federal Information Processing Standard)
Ein vom NIST veröffentlichter Standard der amerikanischen Regierung.

Firewall
Eine Kombination aus Hardware und Software zum Schutz des öffentlichen/privaten Netzwerks gegen bestimmte Angriffe von außen zur Gewährleistung eines bestimmten Maßes an Sicherheit.

Firmenweiter Unterschriftenschlüssel
Ein öffentlicher Schlüssel, der vom Sicherheitsbeauftragten eines Unternehmens als Schlüssel für das ganze System festgelegt wird und den alle Benutzer dieses Unternehmens bei der Unterzeichnung anderer Schlüssel als zuverlässig betrachten können.

Geheimnisteilung
siehe “Teilen von Schlüsseln”.

Gültigkeit
Gibt den Grad der Gewißheit an, mit der der Schlüssel tatsächlich dem angegebenen Eigentümer gehört.

Hash-Funktion
Einweg-Funktion, bei der eine Nachricht beliebiger Länge eingegeben wird und es zu einer Ausgabe fester Länge kommt.

Hexadezimal	Das Hexadezimalsystem ist ein Zahlensystem, das auf der Zahl 16 basiert. Bei diesem System werden 16 aufeinanderfolgende Nummern für jede Stelle einer Zahl verwendet (einschließlich Null), bevor eine weitere Stelle hinzugefügt wird. (Bitte beachten Sie, daß in dieser Erklärung die dezimale Zahl “16” verwendet wird, um die hexadezimale Zahl “10” zu beschreiben.) Die hexadezimalen Zahlen sind 0 bis 9, danach sind die Buchstaben A bis F zu verwenden.
Hierarchisches Vertrauen	Normalerweise eine gestaffelte Reihe von Personen, die Vertrauen strukturiert weitergeben. Wird häufig bei der Festlegung von Zertifizierungsinstanz bei X.509 für ANSI verwendet.
Höhergestellter Schlüsselverwalter	Autorisierter Schlüsselverwalter für autorisierte Schlüsselverwalter.
HTTP (HyperText Transfer Protocol)	Ein Protokoll zum Übertragen von Dokumenten zwischen Servern oder von einem Server zu einem Client.
IDEA (International Data Encryption Standard)	Ein symmetrischer 64-Bit-Blockchiffrierer unter Verwendung von 128-Bit-Schlüsseln. Er basiert auf dem Konzept, Vorgänge aus verschiedenen algebraischen Gruppen zu mischen. Wird als einer der wirksamsten Algorithmen angesehen.
IKE (Internet Key Exchange)	Dient der sicheren Übertragung von Schlüsseln über das Internet. IKE kann auch für Sicherheitsarchitekturen mit IPsec eingesetzt werden.
IKE- und IPsec-Vorschläge	Durch die IKE- und IPsec-Vorschläge weiß PGPnet, welche Vorschläge Sie anderen Benutzern unterbreiten. Vorschläge müssen exakt so wie festgelegt akzeptiert werden. PGPnet läßt dabei sowohl als IKE- als auch als IPsec-Vorschläge mindestens einen und maximal 16 Vorschläge zu.
Implizites Vertrauen	Implizites Vertrauen ist für *Schlüsselpaare* an Ihrem lokalen Schlüsselbund vorgesehen. Falls der private Anteil eines Schlüsselpaares an Ihrem Schlüsselbund gefunden wird, geht PGP davon aus, daß Sie der Eigentümer dieses Schlüsselpaares sind und sich selbst implizit vertrauen.
Integrität	Ein Beleg dafür, daß Daten bei der Speicherung oder Übertragung (durch unbefugte Personen) nicht verändert werden.
IP Spoofing	Einfügen einer falschen Absender-IP-Adresse in eine Internet-Übertragung mit dem Ziel, unberechtigterweise auf ein Computersystem zuzugreifen.

IPCP (IP Payload Compression Protocol)	Protokoll zum Verringern der Größe von IP-Datagrammen. Mit Hilfe dieses Protokolls wird die Kommunikationsgeschwindigkeit zwischen einem Paar kommunizierender Hosts/Gateways (“Knoten”) erhöht, indem die Datagramme komprimiert werden. Voraussetzung dafür ist, daß die Knoten über ausreichend Verarbeitungskapazität verfügen und die Kommunikation über langsame oder überlastete Verbindungen erfolgt. IPPCP sollte nur bei langsamen Verbindungen, wie beispielsweise Modems, verwendet werden; bei schnellen Verbindungen ist es nicht empfehlenswert.
IPsec	Von der IETF in Erwägung gezogenes Verschlüsselungssystem auf TCP/IP-Ebene.
ISO (International Organization for Standardization)	Verantwortlich für viele Standards wie OSI oder den internationalen Standard für ANSI mit X.509.
Klartext	Daten oder Nachrichten in einer für den Menschen lesbaren Form vor dem Verschlüsseln (auch *unverschlüsselter Text* genannt).
Klartextsignierte Nachricht	Nachrichten, die digital signiert, aber nicht verschlüsselt sind.
Komprimierungsfunktion	Eine Komprimierungsfunktion verwendet eine Eingabe fester Länge und gibt eine kürzere Ausgabe mit fester Länge zurück.
Konventionelle Verschlüsselung	Eine Verschlüsselungsmethode, die statt eines öffentlichen Schlüssels eine allgemein bekannte Paßphrase verwendet. Hierbei wird die Datei mit einem Sitzungsschlüssel verschlüsselt, der die Verschlüsselung mit einer angegebenen Paßphrase durchführt.
Kryptoanalyse	Die Kunst oder Wissenschaft des Konvertierens von chiffriertem Text in Klartext ohne anfängliche Kenntnis des für die Verschlüsselung des Textes verwendeten Schlüssels.
Kryptographie	Die Kunst und Wissenschaft des Erstellens von Nachrichten, die eine beliebige Kombination der Attribute “vertraulich”, “unterschrieben”, “unverändert” mit Urheberrechtsnachweis aufweisen.
Kryptographie mit öffentlichen Schlüsseln	Kryptographie, bei der Schlüsselpaare mit jeweils einem öffentlichen und einem privaten Schlüssel verwendet werden. Bei dieser Technik sind keine Sicherheitsvorkehrungen für den Datenübertragungsweg selbst erforderlich.
LDAP (Lightweight Directory Access Protocol)	Ein einfaches Protokoll zur Unterstützung von Zugriff und Suchvorgängen in Verzeichnissen mit Informationen, wie beispielsweise Namen, Telefonnummern und Adressen in sonst inkompatiblen Systemen über das Internet.

MIC (Message Integrity Check)	Wurde anfangs in PEM zur Authentisierung mittels MD2 oder MD5 definiert. Micalg (Message Integrity Calculation) wird in sicheren MIME-Anwendungen eingesetzt.
MIME (Multipurpose Internet Mail Extensions)	Eine frei verfügbare Menge von Spezifikationen, mit denen Text in Sprachen mit verschiedenen Zeichensätzen sowie Multimedia-E-Mails zwischen vielen verschiedenen Computer-Systemen mit Internet-E-Mail-Standards ausgetauscht werden können.
Nachrichtenkern	Ein kompaktes “Destillat” Ihrer E-Mail-Nachricht bzw. Datei-Prüfsumme. Der Nachrichtenkern stellt Ihre E-Mail-Nachricht dar, so daß sich ein anderer Nachrichtenkern ergäbe, wenn die Nachricht in irgendeiner Form verändert würde.
Nur Text	Normaler, lesbarer, unverschlüsselter und nicht unterschriebener Text.
Öffentlicher Schlüssel	Einer der beiden Schlüssel eines Schlüsselpaares. Mit dem öffentlichen Schlüssel werden Informationen verschlüsselt und Unterschriften verifiziert. Der öffentliche Schlüssel eines Benutzers kann an viele bekannte oder unbekannte Personen innerhalb und außerhalb eines Unternehmens weitergegeben werden. Mit Hilfe des öffentlichen Schlüssels einer Person kann niemand an den entsprechenden privaten Schlüssel gelangen.
Öffentlicher Schlüsselbund	Eine Reihe von öffentlichen Schlüsseln. Ihr öffentlicher Schlüsselbund enthält Ihre eigenen öffentlichen Schlüssel.
Paßphrase	Eine einprägsame Wortgruppe, die eine höhere Sicherheit als ein einzelnes Paßwort gewährleistet. Durch “Verwürfeln” von Schlüsseln wird sie in einen Zufallsschlüssel umgewandelt.
Paßwort	Eine Zeichenfolge oder ein Wort, die oder das eine Person zur Authentisierung, Überprüfung oder Verifizierung in ein System eingibt.
PFS (Perfect Forward Secrecy, Höchste Geheimhaltung beim Weiterleiten)	Bei Schlüsselvereinbarungsprotokollen auf der Basis asymmetrischer Kryptographie Eigenschaft, mit der sichergestellt wird, daß ein Sitzungsschlüssel aus einem Satz langfristig gültiger öffentlicher und privater Schlüssel nicht unbefugt entschlüsselt wird, falls einer der privaten Schlüssel in der Zukunft unbefugt entschlüsselt werden sollte.
PGP/MIME	Eine IETF-Norm (RFC 2015) zur Geheimhaltung und Authentisierung unter Verwendung der in RFC1847 erläuterten MIME-Sicherheitsinhaltstypen (Multipurpose Internet Mail Extensions; MIME). PGP/MIME wird momentan in PGP 5.0 und späteren Versionen verwendet.

Phase 1 und Phase 2

Die IKE-Abstimmung erfolgt in zwei Phasen. In Phase 1 authentisieren sich die beiden Parteien und richten eine Schlüsselverwaltungs-SA für den Schutz der Daten ein, die während der Abstimmung übertragen werden. In dieser Phase wird zum Sichern der Nachrichten während der Abstimmung die Schlüsselverwaltungspolitik verwendet. In Phase 2 wird die Datenverwaltungs-SA ausgehandelt, die mit Hilfe der Datenverwaltungspolitik IP-Sicherheitstunnels im Kernel für das Verschlüsseln und Entschlüsseln von Datenpaketen einrichtet.

PKCS (Public Key Crypto Standards)

Gruppe von *De-facto*-Normen zur Verschlüsselung mit öffentlichen Schlüsseln, die in Zusammenarbeit mit einem informellen Konsortium (Apple, DEC, Lotus, Microsoft, MIT, RSA und Sun) entwickelt wurden. Dazu gehören algorithmus-spezifische und von Algorithmen unabhängige Implementierungsnormen. Es handelt sich hierbei um Spezifikationen, die die Nachrichtensyntax definieren, wie auch weitere Protokolle der RSA Data Security Inc.

PKI (Public Key Infrastructure)

Ein weitverbreitetes und zugängliches Zertifikatssystem zum Erhalt von öffentlichen Schlüsseln eines Benutzers, bei dem Sie bis zu einem gewissen Grad sicher sein können, daß Sie den “richtigen” Schlüssel erhalten haben und daß dieser nicht zurückgenommen wurde.

Primärschlüssel (IPsec)

IPsec-Schlüssel für das Erstellen Ihrer Sicherheitsverbindungen. Werte können als zeitliche Werte oder als Datengröße festgelegt werden.

Privater Schlüssel

Der geheime Teil eines Schlüsselpaares, mit dem Informationen unterschrieben und entschlüsselt werden. Der private Schlüssel eines Benutzers sollte geheim gehalten werden und nur diesem bekannt sein.

Privater Schlüsselbund

Ein Satz aus einem oder mehreren privaten Schlüsseln, die alle dem Eigentümer des privaten Schlüsselbundes gehören.

RFC (Request for Comment, Bitte um Kommentar)

Ein IETF-Dokument, aus der Untergruppe FYI RFC (geben Überblicke und Einführungen) oder aus der Untergruppe STD RFC (geben Internet-Normen an). Die Abkürzung FYI steht für “For Your Information” (Zu Ihrer Information). Jede RFC wird anhand ihrer jeweiligen RFC-Nummer indiziert. Über diese Nummer kann die RFC auch abgerufen werden (www.ietf.org).

RSA

Abkürzung von RSA Data Security, Inc. Steht auch für die Firmenchefs Ron Rivest, Adi Shamir und Len Adleman oder bezieht sich auf den von ihnen erfundenen Algorithmus. Der RSA-Algorithmus wird in der Kryptographie mit öffentlichen Schlüsseln verwendet. Seine Funktionsweise beruht auf der Tatsache, daß zwei große Primzahlen zwar leicht miteinander zu multiplizieren sind, aber das Produkt nur schwer wieder in sie zu zerlegen ist.

S/MIME (Secure Multipurpose Mail Extension)	Ein von Deming Software und RSA Data Security entwickelter Normvorschlag zum Verschlüsseln und/oder zur Authentisierung von MIME-Daten. S/MIME definiert ein Format für MIME-Daten, die Algorithmen, die für die übergreifende Funktionalität verwendet werden müssen (RSA, RC2 und SHA-1), sowie für zusätzliche betriebstechnische Belange wie ANSI X.509-Zertifikate und Übertragung im Internet.
SA (Security Association, Sicherheitsverbindung)	Beziehung zwischen zwei oder mehr Entitäten, die beschreibt, wie die Entitäten die Sicherheitsservices für die sichere Kommunikation verwenden.
Schlüssel	Digitaler Code zur Verschlüsselung und Unterzeichnung sowie zur Entschlüsselung und Verifizierung von E-Mail-Nachrichten und Dateien. Schlüssel werden paarweise erstellt und in Schlüsselbunden gespeichert.
Schlüsselaustausch	Ein Schema mit zwei oder mehreren Knoten zum Übertragen eines geheimen Sitzungsschlüssels über einen nicht gesicherten Kanal.
Schlüsselbund	Eine Reihe von Schlüsseln. Jeder Benutzer verfügt über zwei Arten von Schlüsselbunden: einen privaten Schlüsselbund und einen öffentlichen Schlüsselbund.
Schlüsselhinterlegung/ -wiederherstellung	Ein Verfahren, bei dem der Benutzer eines Verschlüsselungssystems mit öffentlichen Schlüsseln seinen privaten Schlüssel an einen Dritten übergibt, so daß dieser den Austausch von verschlüsselten E-Mail-Nachrichten überwachen kann.
Schlüssel-ID	Ein lesbarer Code, mit dem ein Schlüsselpaar eindeutig identifiziert wird. Zwei Schlüsselpaare können dieselbe Benutzer-ID haben, die Schlüssel-IDs sind jedoch stets verschieden.
Schlüssellänge	Die Anzahl der Bits zur Darstellung der Schlüsselgröße. Je länger der Schlüssel, desto stärker ist er.
Schlüsselpaar	Ein öffentlicher und der zugehörige private Schlüssel. In Kryptographiesystemen mit öffentlichen Schlüsseln (wie PGP) verfügt jeder Benutzer über mindestens ein Schlüsselpaar.
Schlüsselverwalter	Eine Person oder ein Unternehmen mit der Erlaubnis, sich für die Echtheit der öffentlichen Schlüssel anderer Benutzer zu verbürgen. Sie können einen Schlüsselverwalter festlegen, indem Sie seinen öffentlichen Schlüssel unterschreiben.
Schlüsselverwaltung	Das Verfahren zum sicheren Speichern und Verteilen akkurater kryptographischer Schlüssel. Der Gesamtprozeß des sicheren Erstellens und Verteilens von kryptographischen Schlüsseln an befugte Empfänger.
Selbstunterschriebener Schlüssel	Ein öffentlicher Schlüssel, der vom entsprechenden privaten Schlüssel zum Nachweis des Eigentumsrechts unterschrieben wurde.

Sicherer Kanal	Ein Mittel zur Übertragung von Informationen zwischen Terminals, bei der kein Gegner diese Informationen umstellen, löschen, lesen oder andere Informationen einfügen kann (SSL, IPsec, “Ins-Ohr-Flüstern”)
Sitzungsschlüssel	Der geheime (symmetrische) Schlüssel zum Verschlüsseln aller Datensätze auf Transaktionsbasis. Für jede Kommunikationssitzung wird ein anderer Sitzungsschlüssel verwendet.
SSL (SSL-Protokoll, Secure Socket Layer)	Wurde von Netscape zur Gewährleistung von Sicherheit und zur Geheimhaltung im Internet entwickelt. SSL unterstützt die Server- und Client-Authentisierung und verwaltet Sicherheit und Integrität des Übertragungskanals. Wirkt auf der Übertragungsebene und dient als “Socket-Bibliothek”, wodurch eine anwendungsunabhängige Wirkungsweise ermöglicht wird. Mit Hilfe von SSL wird der gesamte Kommunikationskanal verschlüsselt, digitale Unterschriften auf Nachrichtenebene werden jedoch nicht unterstützt.
Symmetrischer Algorithmus	Anderweitig bekannt als konventioneller geheimer Schlüssel und Einzelschlüsselalgorithmus. Die Schlüssel für die Ver- und Entschlüsselung sind entweder identisch oder können basierend auf dem jeweils anderen berechnet werden. Es gibt zwei Unterkategorien – Block und Strom.
Teilen von Schlüsseln oder “Geheimnisverteilung”	Ein Vorgang, bei dem ein privater Schlüssel in viele Teile zerlegt und an mehrere Personen verteilt wird. Zur Verwendung des Schlüssels muß eine festgelegte Anzahl an Personen ihre Schlüsselteile zusammensetzen.
Teilschlüssel	Unter einem Teilschlüssel versteht man einen Diffie-Hellman-Verschlüsselungsschlüssel, der dem Masterschlüssel als Teilmenge hinzugefügt wird. Nach der Erstellung eines Teilschlüssels können Sie diesen ungültig werden lassen oder zurücknehmen, ohne daß der Masterschlüssel oder die darauf gesammelten Unterschriften hierdurch beeinflußt werden.
Text	Druckbarer ASCII-Standardzeichensatz mit 7-Bit.
TLS (Transport Layer Security)	Ein IETF-Entwurf. Version 1 basiert auf Version 3.0 des SSL-Protokolls (Secure Sockets Layer; SSL) und dient zur Wahrung der Privatsphäre bei der Kommunikation über das Internet.
TLSP (Transport Layer Security Protocol)	ISO 10736, Entwurf des internationalen Standards.
Triple-DES	Eine Verschlüsselungskonfiguration, in der der DES-Algorithmus dreimal mit drei unterschiedlichen Schlüsseln verwendet wird.

Twofish

Neuer, von Bruce Schneier entwickelter symmetrischer 256-Bit-Blockverschlüsselungsalgorithmus. Er ist einer von fünf Algorithmen, die vom US-amerikanischen National Institute of Standards and Technology (NIST) als Ersatz für den aktuellen Advanced Encryption Standard (AES) in Betracht gezogen werden.

Übernahme einer TCP-Sitzung

Findet statt, wenn ein Hacker die Kontrolle über eine TCP-Sitzung zwischen zwei Rechnern übernimmt. Da die meisten Authentisierungen nur zu Beginn einer TCP-Sitzung auftreten, ist der Hacker damit in der Lage, auf einen Rechner zuzugreifen.

Unterschreiben

Eine Unterschrift leisten.

Unterschrift

Ein digitaler, mit einem privaten Schlüssel erstellter Code. Unterschriften ermöglichen im Prozeß der Unterschriftsverifizierung die Authentisierung von Informationen. Wenn Sie eine E-Mail-Nachricht oder eine Datei unterschreiben, erstellt PGP mit Ihrem privaten Schlüssel einen digitalen Code, der sowohl für den Inhalt der Nachricht als auch für Ihren privaten Schlüssel eindeutig ist. Jeder kann mit Ihrem öffentlichen Schlüssel Ihre Unterschrift verifizieren.

Urheberrechtsnachweis

Verhindert die Verweigerung von früheren Verpflichtungen oder Leugnung von Handlungen.

Verifizierung

Das Vergleichen einer mit Hilfe eines privaten Schlüssels erstellten Unterschrift mit dem entsprechenden öffentlichen Schlüssel. Die Verifizierung beweist, daß die Informationen tatsächlich vom Unterzeichner gesendet wurden und daß die E-Mail-Nachricht nicht nachträglich von einer dritten Person verändert wurde.

Verschlüsselung

Eine Methode zum Chiffrieren von Informationen, um sie für jeden außer für den gewünschten Empfänger unlesbar zu machen

Verschlüsselungssystem

Ein System, das aus kryptographischen Algorithmen, beliebigem Klartext, chiffriertem Text und Schlüsseln besteht.

Vertrauenswürdig

Ein öffentlicher Schlüssel kann von Ihnen als vertrauenswürdig betrachtet werden, wenn er von Ihnen oder einer anderen Person, die Sie als Schlüsselverwalter festgelegt haben, zertifiziert wurde.

Virtuelle Identität

Die virtuelle Identität von PGPnet basiert auf dem von den IPsec-Arbeitsgruppen der IETF entworfenen config-mode-Standard. Sie wird auch als Phase 1.5 und Transaktionsvermittlung bezeichnet.

Diese Funktion kann von einem sicheren Gateway aus IP-Adressen und weitere Konfigurationsinformationen für Ihren Computer abrufen. Da der Gateway Ihrem Computer eine Adresse zuweist, werden Sie von allen Computern hinter dem Gateway als Teil Ihres Netzwerks angesehen, und sie können ungehindert mit Ihnen kommunizieren.

Vollmacht	Übertragen von offiziellen Genehmigungen, Zugriffsrechten oder juristischen Vollmachten an einen Benutzer.
Vollmachtszertifikat	Elektronisches Dokument, das als Bestätigung des Vorhandenseins von Zugriffsrechten sowie der angeblichen Identität von Benutzern dient.
VPN (Virtual Private Network)	Ermöglicht die Ausdehnung von privaten Netzwerken vom Endbenutzer über ein öffentliches Netzwerk (Internet) direkt bis zum Home-Gateway Ihrer Wahl, wie beispielsweise zum Intranet Ihrer Firma.
VPN-Schlüsselaktualisierung	Für die Erstellung Ihrer Sicherheitsverbindungen werden die Einrichtungsschlüssel (IKE) und die Primärschlüssel (IPsec) herangezogen. Diese werden auf der Grundlage der auf der Registerkarte “VPN-Optionen” (Mac) festgelegten Werte für “VPN-Schlüsselaktualisierung” automatisch erneuert.
Web of Trust	Modell des verteilten Vertrauens, mit dem PGP den Eigentümer eines öffentlichen Schlüssels bestimmt. Der Grad des Vertrauens ist kumulativ und basiert auf der Kenntnis einer Person über die Schlüsselverwalter.
Wörterbuch-Angriff	Berechneter schwerer Angriff zum Entschlüsseln eines Paßworts durch Testen von offensichtlichen und logischen Wortkombinationen.
X.509	Digitales ITU-T-Zertifikat, bei dem es sich um ein international anerkanntes elektronisches Dokument zur Prüfung der Identität und der Eigentümer von öffentlichen Schlüsseln in einem Kommunikationsnetzwerk handelt. Es enthält den Name der Person, die das Zertifikat ausgestellt hat, Informationen zur Identifizierung des Benutzers sowie die digitale Unterschrift des Ausstellers. Außerdem sind weitere mögliche Erweiterungen enthalten.
Zeitangaben	Aufzeichnen der Erstellungszeit oder der Zeit des Vorhandenseins von Informationen.
Zertifikat (digitales Zertifikat)	Von einem vertrauenswürdigen Dritten mit einem öffentlichen Schlüssel verbundenes elektronisches Dokument, das beweist, daß der öffentliche Schlüssel einem rechtmäßigen Eigentümer gehört und nicht verfälscht wurde.
Zertifizieren	Den öffentlichen Schlüssel einer anderen Person unterschreiben.
Zertifizierung	Bestätigung von Informationen durch einen vertrauenswürdigen Benutzer.
Zertifizierungsinstanz	Eine oder mehrere vertrauenswürdige Personen, denen die Verantwortung zugewiesen wird, den Ursprung von Schlüsseln zu zertifizieren und diese einer allgemein zugänglichen Datenbank hinzuzufügen.

Zufallszahl	Ein wichtiger Aspekt für viele Verschlüsselungssysteme sowie ein notwendiges Element beim Erzeugen von eindeutigen Schlüsseln, die für Gegner nicht berechenbar sind. Echte willkürliche Zahlen werden normalerweise von analogen Quellen abgeleitet und machen üblicherweise den Einsatz spezieller Hardware erforderlich.
Zurücknahme	Widerrufen von Zertifizierungen oder Bevollmächtigungen.

Index

A

Abfangangriff ("man-in-the-middle-attack") 63

Abrufen

- X.509-Zertifikat 95

Abrufen der virtuellen Identität für diesen Gateway aktivieren (Option) 232

Adapter einstellen:

- sichere Netzwerkschnittstelle ändern 198

AES (Advanced Encryption Standard)

- Definition 305

AH (Authentication Header)

- Definition 305

Algorithmus

- CAST 260, 306
- DES 307
- Diffie-Hellman 307
- DSA 307
- Hash 305
- IDEA 260, 309
- RSA 312
- symmetrisch 314
- Triple-DES 260, 314
- Twofish 260, 315
- Verschlüsselung 305

Ändern

- eigene Paßphrase 81
- Firewall-Regeln 202
- Host 233
- sichere Netzwerkschnittstelle 198
- sicherer Gateway 233
- Teilnetz 233

Angriffe 293

- Abfangangriff 63
- aufspüren 195
- Beschreibungen 293
- durch Sichern Ihrer Schlüssel vor Angriffen schützen 51

Angriffe aufspüren

- Quelle aufzeichnen (Funktion) 195

Anonymität

- Definition 305

ANSI (American National Standards Institute)

- Definition 305

Antwort-Timeout 288

Anzeigen

- abgelaufene SAs 189
- aktive SAs 189
- Details zu blockierten Hosts 194
- Schlüsselattribute 46
- Schlüsselbundattribute 68–72
- Schlüsselpaar aus priv. und öff. Schlüssel 36
- Status (Registerkarte in PGPnet) 189
- was verschlüsselt wurde 245

Arbeit produktiver gestalten

- Tastaturbefehle (Hotkeys) 37

ASCII-Text

- Definition 305

Asymmetrische Schlüssel

- Definition 305

Attribute

- des Schlüsselbundes ändern 68–72
- des Schlüsselbundes anzeigen 68–72

Aufspüren der Quelle von Paketen 201
Ausführen
PGP 36
Ausführen von PGP 36
Aussprechen
Vertrauen für Schlüsselüberprüfungen 80
Austauschen
öffentliche Schlüssel 31, 55
über ICQ 140
von anderen Benutzern erhalten 58–62
PGPdisk-Volumes 164
Authentisieren
PGP-Schlüssel verwenden 267
X.509-Zertifikate verwenden 267
Authentisierung
Definition 305
Automatisch
PGPdisk-Volumes entladen 161
PGPdisk-Volumes laden 152, 162
Automatisch entladen (Voreinstellung)
im Standby-Modus des Computers 281
nach x Minuten ohne Aktivität 161, 280
Automatische Schlüsselerneuerung
Definition 306, 316
für Primärschlüssel (IPsec) festlegen 266
für Setup-Schlüssel (IKE) festlegen 266
Automatisches
Entladen von PGPdisk-Volumes 280, 281
Autorisierter Schlüsselverwalter 65
Definition 306

B

Back Orifice
Angriff, Beschreibung 293
Definition 306
Backdoor
Definition 306
Bearbeiten
Host, Teilnetz oder Gateway 233
Hosteintrag
Host auffordern, einen speziellen Schlüssel vorzulegen 237
Liste der benutzerdefinierten Firewall-Schutzregeln 215
Beenden
PGPnet 183, 184
SA vom PGPnet-Menü in PGPtray 186
Bei Angriffen akustisches Signal ausgeben (Option)
persönliches IDS 219
Beliebiger gültiger Schlüssel (Option) 237
Benutzerdefinierte Firewall-Schutzregeln
allgemeine Informationen 201
entfernen 214
erstellen 211
Priorität ändern 215
Benutzerdefinierter Firewall-Schutzgrad
erstellen 210
Benutzerdefinierter Schlüssel
erstellen 46
Benutzer-ID
Definition 306
Bereinigen von freiem Speicherplatz 132
Tasks planen 136
Beschreibung der Angriffe 293
Bevorzugter Algorithmus 259, 260
Blinde Unterschrift
Definition 306
Blockieren von Datenpaketen 202
Blockieren von Datenverkehr 201

Blockierter Host 194
aus Liste entfernen 194, 197
Blockierter Host (Dialogfeld) 195
Blockverschlüsselung
Definition 306
Bonk, Angriff 293

C

CA. Siehe “Zertifizierungsinstanz”
CAPI (Crypto API)
Definition 306
CAST-Algorithmus 260
Definition 306
Certificate Server. Siehe “Schlüsselserver”
Chiffrierter Text
Definition 307
Chiffrierungen
bestimmte Chiffrierungen in PGPnet zulassen 272, 273
CRYPTOKI
Definition 307

D

Dateien
löschen 132
öffentliche Schlüssel importieren 61
öffentlichen Schlüssel exportieren 57
unwiederherst. löschen 132
Datenintegrität
Definition 307
Deaktivierter Expert-Modus 234
Denial-of-Service-Angriff
Definition 307
DES (Data Encryption Standard)-Algorithmus
Definition 307
Details zu blockierten Hosts
anzeigen 194
Diffie-Hellman / DSS-Verfahren
Schlüssel erstellen 47
Diffie-Hellman-Algorithmus
Definition 307
Digitale Unterschrift
Definition 307
löschen 73
und Echtheit 64
Digitalgeld
Definition 307
Direktes Vertrauen
Definition 307
DNS-Suche
Einbrecher (Registerkarte) 195
IP-Adresse eines Hosts suchen 236
verwenden 236
DNS-Suche (Funktion) 194
DSA (Digital Signature Algorithm)
Definition 307
DSS (Digital Signature Standard)-Algorithmus
Definition 307

E

ECC (Elliptic Curve Cryptosystem)
Definition 307
EES (Escrowed Encryption Standard)
Definition 307
Eigenschaften
Einbrecher (Registerkarte) 194
Status (Registerkarte) 190
Einbrecher (Registerkarte) 187, 193
Eigenschaften 194

Einrichtungsschlüssel
Definition 307
Einweg-Hash
Definition 308
Elgamal-Schema
Definition 308
E-Mail
eigenen öffentlichen Schlüssel einfügen 57
E-Mail-Plugin hinzufügen 112
Empfängergruppen erstellen 122
Empfängergruppen löschen 122
Empfängergruppen verknüpfen 123
entschlüsseln 124, 126
öffentliche Schlüssel kopieren 61
private E-Mail-Nachrichten empfangen 111
private E-Mail-Nachrichten senden 111
unterschreiben 32, 111, 123
verifizieren 124, 126
verschlüsseln 32, 111, 123
für Gruppen 121
E-Mail-Programme
PGP verwenden 37
Empfangen
private E-Mail-Nachrichten 111
Empfänger
Gruppen 121
Empfängergruppen
erstellen 122
Gruppen löschen 122
Gruppen verknüpfen 123
löschen 122
Endg. löschen
verwenden 132
Endgültig löschen
Festplatten 132, 136
Free Space Wiper verwenden 132
Entfernen
benutzerdefinierte Firewall-Schutzregeln 214
Dateien m. d. Funktion “Endgültig löschen” 132
Gateways 233
Host aus der Liste der blockierten Hosts 194, 197
Hosts 233
SAs 190
Schlüssel vom Server 55
Teilnetze 233
Entfernte Authentisierung 237
Entkomprimieren-Komprimierung
und PGPnet 272
Entladen von PGPdisk-Volumes 159
automatisch 161
Entschlüsseln
E-Mail 124
ICQ-Nachrichten 139
mit geteilten Schlüsseln 132
mit PGPmenu 131
mit PGPtray 131
über die Zwischenablage 36
Entschlüsselung
Definition 308
Ereignisse anzeigen 197
Protokoll (Registerkarte) 197
Erhalten
öffentliche Schlüssel anderer Benutzer 58–62
Erstellen
Empfängergruppen 122

Schlüsselpaar aus privatem und öffentlichem Schlüssel 43–46
Teilschlüssel 55
Erweitert (Schaltfläche)
Registerkarte “Protokoll” 289
Erweiterte Optionen 259
Exportformat 262
Sicherung des Schlüsselbundes 262
Vertrauensmodell 261
Erweitertes Protokoll 197
Erzeugen
Schlüsselpaare
Optionen festlegen 246
ESP (Encapsulating Security Payload)
Definition 308
Eudora 112, 124
mit PGP/MIME 124
ohne PGP/MIME 126
Exchange/Outlook 112
Expert-Modus
Host auffordern, einen speziellen Schlüssel vorzulegen 237
vom PGP-Administrator deaktiviert 234
zum Hinzufügen von Hosts, Gateways und Teilnetzen 234
Explorer
PGP verwenden 35
Exportformat
für das Exportieren von Schlüsseln 262
Exportieren
Schlüssel in Dateien 57

F

Fehlermeldungen 287
Festlegen
Paßphrase für einen Schlüssel 44, 108
PGP-Optionen 244
Schlüsselgültigkeitswerte 265
Werte für die automatische Schlüsselerneuerung 266
Festplatten
automatisches Bereinigen einrichten 136
Dateien endg. löschen v. 132
freien Speicherplatz bereinigen 132
Fingerabdrücke
Definition 308
überprüfen 91
vergleichen 63
FIPS (Federal Information Processing Standard)
Definition 308
Firewall
benutzerdefinierte Firewall-Regeln 211
benutzerdefinierter Firewall-Schutzgrad 210
Definition 308
konfigurieren 202
Priorität der Regeln ändern 215
Schutzregeln entfernen 214
vordefinierte Schutzgrade 203
Firmenweiter Unterschriftenschlüssel 308
Foto-ID
zu einem Schlüssel hinzufügen 49
Fraggle, Angriff 293
Free Space Wiper verwenden 132, 136

G

Gateways
ändern 233
Definition 179

entfernen 233
Geheimnisteilung
Definition 308
Gemeinsame Paßphrase einstellen (Option) 237
Gemeinsames Geheimnis 237
Gruppen
erstellen 122
Gruppen verknüpfen 123
löschen 122
Mitglieder hinzufügen 122
Gruppenlisten 256
Gültigkeit
Definition 308
Schlüsselgültigkeitswerte festlegen 265
von Schlüsseln überprüfen 62
Gültigkeitsebene
ungültig 262
zweitrangige 262

H

Hash-Funktionen
Definition 308
in PGPnet zulassen 272, 273
Hexadezimal
Definition 309
Hierarchisches Vertrauen
Definition 309
Hilfe
aufrufen 36
Hinzufügen 194
E-Mail-Plugin
ICQ-Plugin 112
Foto-ID zu einem Schlüssel 49
Gruppen verknüpfen 123
Host 227, 234
Host zur Liste der blockierten Hosts 194
Root-CA-Zertifikat Ihrem Schlüssel 92
sicheren Gateway 234
Teilnetz 234
X.509-Zertifikat 258
Höchste Geheimhaltung beim Weiterleiten (Perfect Forward Secrecy (PFS)) 275
Höhergestellter Schlüsselverwalter 65
Definition 309
Host auffordern, einen speziellen Schlüssel vorzulegen 237
Host exportieren 193
Host / Gateway
Host auffordern, einen speziellen Schlüssel vorzulegen 237
Hosts
ändern 233
Anzeige im PGPnet-Menü in PGPtray 186
entfernen 233
exportieren 193
hinzufügen 227
importieren 193
IP-Adresse suchen 236
SA beenden 192
SAs einrichten 192
Hotkey
Aktuelles Fenster entschlüsseln und verifizieren (Option) 254
Aktuelles Fenster unterschreiben 254
Aktuelles Fenster verschlüsseln 254
Aktuelles Fenster verschlüsseln und unterschreiben 254
Alle PGPdisks entladen 254
Optionen festlegen 253

Zwischenspeicher für Paßphrasen leeren 254
HotKey zum Entladen von PGPdisks festlegen 281
HTTP (HyperText Transfer Protocol)
Definition 309

I

ICQ
Nachrichten entschlüsseln 139
Nachrichten verschlüsseln 141
Schlüssel austauschen 140
IDEA (International Data Encryption Standard)-Algorithmus
Definition 309
für die Verschlüsselung 260
IDS, erkannte Angriffe 293
IKE (Internet Key Exchange)
Definition 309
Verhandlung, Beschreibung 181
Vorschläge
Definition 309
hinzufügen 276
Implizites Vertrauen
Definition 309
Importieren
Hosts in PGPnet 193
öffentliche Schlüssel aus Dateien 61
private PKCS-12-X.509-Schlüssel 62
private Schlüssel 62
Initialisieren
SA 181
SA vom PGPnet-Menü in PGPtray 186
Integrität
Definition 309
Internet Key Exchange. Siehe “IKE”.
IP Spoofing
Angriff, Beschreibung 293
Definition 309
IP-Adresse
mit DNS-Suche suchen 236
IPPCP (IP Payload Compression Protocol)
Definition 310
IPsec
Definition 179, 310
Vorschläge
Definition 309
hinzufügen 276
ISO (International Organization for Standardization)
Definition 310

J

Jolt, Angriff 294
Jolt2, Angriff 294

K

Kein SPI gefunden 287
Kein Vorschlag ausgewählt 288
Keine SA gefunden 287
Klartext
Definition 310
Klartextsignierte Nachricht
Definition 310
Kommunikation blockieren 193, 195
persönliches IDS 218
Komprimierungsfunktion
Definition 310
in PGPnet zulässige 272
Konventionelle Verschlüsselung 116, 119, 131

Definition 310

Kryptoanalyse

Definition 310

Kryptographie

Definition 310

Kryptographie mit öffentlichen Schlüsseln

Definition 310

Kundendienst

Adressen und Telefonnummern 20

L

Laden von PGPdisk-Volumes 158

auf einem entfernten Server 163

automatisch 152, 162

Land, Angriff 294

LDAP (Lightweight Directory Access Protocol)

Definition 310

Legitimität

von Schlüsseln bestimmen 62

Löschen

Benutzer-IDs 73

Dateien 132

digitale Unterschriften 73

Empfängergruppen 122

m. d. Funktion “Endgültig löschen” 132

SAs 190

Schlüssel 73

Schlüssel vom Server 55

Unterschriften vom Server 55

Löschen von Protokollinformationen 198

Lotus Notes 112

Nachrichten entschlüsseln und verifizieren 125

unterschreiben mit 117

verschlüsseln mit 117

LZS-Komprimierung

und PGPnet 272

M

MD5 Hash

und PGPnet 272

MIC (Message Integrity Check)

Definition 311

MIME-Standard

Definition 311

E-Mail-Nachrichten entschlüsseln 124, 126

E-Mail-Nachrichten verschlüsseln 115, 118

Modi

Expert 234

N

Nachrichtenkern

Definition 311

NAT-Inkompatibilität wurde erkannt 288

Nestea, Angriff 294

Net Tools PKI Server 93

Network Associates

Adressen und Telefonnummern

Kundendienst 20

Netzwerkkarte, sichern 199

Netzwerkverkehr

blockieren 202

Nicht von einer Regel erfaßter Verkehr 202

O

Öffentliche Schlüssel

an andere Benutzer verteilen 55

an andere Benutzer weitergeben 31
an Schlüsselserver senden 55
aus Dateien importieren 61
aus E-Mail-Nachrichten kopieren 61
Definition 311
eigenen Schlüssel anz. 36
in Dateien exportieren 57
in eine E-Mail-Nachricht einfügen 57
mit anderen Benutzern austauschen 31, 55
Schlüsselserver durchsuchen 59
schützen 51
speichern 51
Speicherort 67
überprüfen 31
unterschreiben 78
von anderen Benutzern erhalten 31, 58–62
von einem Schlüsselserver holen 59
Vorteile des Sendens an einen Schlüsselserver 55
weitergeben 55
zertifizieren 31
Öffentlicher Schlüsselbund
Definition 311
Öffnen
PGPkeys-Fenster 36
Online-Hilfe
aufrufen 36
Optionen 258
allgemeine 244
CA (Certificate Authority) 258
Datei 248
E-Mail 250
erweitert 259
festlegen 244
Hotkey 253
persönliche Firewall 263
persönliches IDS 263
PGPdisk 279
Schlüsselerzeugung 246
Server, Schlüsselserver 255
Verschlüsselung 245
VPN 263
VPN – Erweitert 270
VPN-Authentisierung 267
Ordner bereinigen
planen 136
Outlook Express 112

P

Paßphrase
ändern 81
Definition 311
festlegen 44, 108
für ein PGPdisk-Volume ändern 153
vergessen 52
vergessene 107
Vorschläge 108
Vorschläge für die Auswahl 45
zum Schutz der PGPdisk 153
Paßwort
Definition 311
Perfect Forward Secrecy (PFS)
Definition 311
Persönliche Firewall
benutzerdefinierte Firewall-Schutzregeln 211
benutzerdefinierter Firewall-Schutzgrad 210
konfigurieren 202

Priorität der Regeln ändern 215
Schutzregeln entfernen 214
vordefinierte Schutzgrade 203
Persönliches IDS
Bei Angriffen akustisches Signal ausgeben (Option) 219
konfigurieren 216
PGPtray-Symbol bei Angriff blinken lassen (Option) 219
Server für ausgehende Mail (SMTP) 219
Verkehr blockieren 218
Persönliches IDS konfigurieren 216
PFS (Perfect Forwared Secrecy). Siehe "Höchste Geheimhaltung beim Weiterleiten"
PGP
mit PGP-Plugins für E-Mail-Programme 37
Problembehebung 283
über das PGPtools-Fenster verwenden 34
über das Systemfeld 36
über die Zwischenablage verwenden 36
Voreinstellungen festlegen 36
PGP Free Space Wiper
verwenden 132
PGP / MIME-Standard
Definition 311
E-Mail-Nachrichten entschlüsseln 124, 126
E-Mail-Nachrichten verschlüsseln 115, 118
Überblick 111
PGPdisk 143–171
CAST (Verschlüsselungsalgorithmus) 168
Sicherheitsvorkehrungen 169
Twofish (Verschlüsselungsalgorithmus) 168
PGPdisk-Einstellungen
automatisch entladen 161
Automatisch entladen (Option) 280, 281
HotKey zum Entladen 281
PGPdisk-Volumes
austauschen 164
automatisch entladen 161, 280, 281
entladen 158, 159
ineinander betten 168
laden 158
Sicherungskopien erstellen 163
PGPdisk-Volumes entladen
automatisch 280
PGPkeys-Fenster
Erstellung (Spaltenüberschrift) 72
Größe (Überschrift) 71
Gültigkeit (Überschrift) 70
öffnen 36
Schlüsseleigenschaften überprüfen 75
Schlüssel-ID 85
Vertrauen (Spaltenüberschrift) 72
verwenden 67
PGPmenu
verwenden 131
PGPnet
beenden 183, 184
deaktivieren 183
Fehlermeldungen 287
PGP-Schlüssel verwenden mit 224
Registerkarte "Status" anzeigen 189
starten 183, 222
Statusleiste 188
Vorschläge festlegen 273

X.509 96

Zulässige entfernte Vorschläge (Option) 272, 273

PGPnet beenden 183

PGPnet-Fenster

Ansicht (Menü) 186

Datei (Menü) 186

Einbrecher (Registerkarte) 187

Erweitert (Registerkarte) 270

Funktionen 186

Hilfe (Menü) 186

Protokoll (Registerkarte) 187

Status (Registerkarte) 187

VPN (Registerkarte) 187

PGP-Schlüssel

für Verbindungsauthentisierung verwenden 267

zum Einrichten einer SA verwenden 224

PGP-Schlüsselerzeugungsassistent

Schlüsselpaare erstellen 43–46

PGPtools

Free Space Wiper verwenden 132

PGP über PGPtools verwenden 34

PGPtray

starten 36

verwenden 131

PGPtray-Symbol bei Angriff blinken lassen (Option)

persönliches IDS 219

Phase 1 und 2

Definition 312

Ping Flood, Angriff 294

Ping of Death, Angriff 294

PKCS (Public Key Crypto Standards)

Definition 312

PKCS-12-Schlüssel

erhalten 62

PKI (Public Key Infrastructure)

Definition 312

Planen

Free Space Wiper 136

freien Speicherplatz bereinigen 136

Ordner bereinigen 136

Port Scanning, Angriff 295

Primärschlüssel

Definition 312

Priv. Schlüssel

eigenen Schlüssel anz. 36

Private Schlüssel

Definition 312

mit dem PGP-Schlüsselerzeugungsassistenten erstellen 43, 46

PKCS-12 X.509 importieren 62

schützen 51

speichern 51

Speicherort 67

Privater Schlüsselbund

Definition 312

Problembehebung

PGP 283

PGPnet 287

Produktives Arbeiten

Tastaturbefehle (Hotkeys) 37

Protokoll (Registerkarte) 187

Ereignisse anzeigen 197

erweitert 197

Protokollinformationen

löschen 198

speichern 198

Q

Quelle aufzeichnen (Funktion) 193, 195

R

Rekonstruieren von Schlüsseln 52, 107
RFC (Request for Comment, Bitte um Kommentar)
Definition 312
Root-CA-Zertifikate 92
zum Schlüsselbund hinzufügen 96
RSA-Algorithmus
Definition 312
RSA-Verfahren
Schlüssel erstellen 47
Rücknahmeschlüssel
Schlüsseleigenschaften anzeigen 87

S

S/MIME (Secure Multipurpose Mail Extension)
Definition 313
SA (Security Association, Sicherheitsverbindung)
Definition 313
SA-Eigenschaften überprüfen 190
Schlüssel
auf einem Schlüsselserver aktualisieren 104
auf Servern wieder erscheinen 107
Benutzernamen entfernen 105
Definition 313
Echtheit verifizieren 62
erzeugen 41
Fingerabdrücke überprüfen 91
Foto-ID hinzufügen 49
geteilten Schlüssel zusammensetzen 99
Größe festlegen 48, 86
löschen 73
rekonstruieren 52, 107
schützen 51
Sicherungskopien erstellen 51
speichern 51
teilen 55
Überblick 41
überprüfen 46
unterschreiben 78
Unterschriften entfernen 105
verloren 52
verlorene 107
Vertrauen für Überprüfungen aussprechen 80
verwalten 67, 244
vom Server löschen 55
weitergeben 55
zurücknehmen 90
Schlüsselaustausch
Definition 313
Schlüsselbunde
anderswo speichern 67
Attribute ändern 68–72
Attribute anzeigen 68–72
Beschreibung 67
Definition 313
Speicherort 67
Schlüsselfingerabdruck
Definition 308
Schlüsselgröße
Diffie-Hellman-Anteil 48
DSS-Anteil 48
festlegen 48, 86
Kompromisse 48, 86

Schlüsselgültigkeitswerte
festlegen 265
Schlüsselhinterlegung/-wiederherstellung
Definition 313
Schlüssel-ID
Definition 313
Eigenschaften 85
Schlüssellänge
Definition 313
Schlüsselpaar
anzeigen 36
Definition 313
eigenes Schlüsselpaar anz. 36
mit dem PGP-Schlüsselerzeugungsassistenten erstellen 43–46
Standard festlegen 73
teilen 55
überprüfen 46
Schlüsselrekonstruktionsserver
Definition 52
Schlüssel senden zum 53
Schlüssel wiederherstellen vom 107
Schlüsselserver
Als Root 256
durchsuchen 59
eigenen Schlüssel auf Server aktualisieren 104
hinzufügen 257
öffentlichen Schlüssel einer Person abrufen 59
öffentlichen Schlüssel senden an 55
Optionen festlegen 255
Schlüssel löschen 55
synchronisieren 256
verwenden, um zurückgenommene Schlüssel in Umlauf zu bringen 90
Schlüsselverwalter
Definition 313
Schlüsselverwaltung
Definition 313
Schützen
eigene Schlüssel 51
Selbstentschlüsselndes Archiv 131
Selbstunterschriebener Schlüssel
Definition 313
Senden
private E-Mail-Nachrichten 111
Server
PGPdisk-Volumes laden 163
Server für ausgehende Mail (SMTP)
persönliches IDS 219
Server. Siehe auch “Schlüsselserver”
SHA-1 Hash
und PGPnet 272
Sichere Darstellung
E-Mail-Verschlüsselungsoption 113
mit früheren Versionen 116
Sichere Hosts
Definition 179
hinzufügen 227
Sichere Netzwerkschnittstelle, ändern 198
Sicherer Kanal
Definition 314
Sicheres Gateway
Definition 180
Sicheres Teilnetz
Definition 180
Sicherheitsverbindung (Security Association, SA)

abgelaufene SAs anzeigen 189
aktive SAs anzeigen 189
aktive SAs speichern 190
Eigenschaften 190
mit Host beenden 192
mit Host einrichten 192
mit PGP-Schlüsseln einrichten 224
SAs entfernen 190
vom PGPnet-Menü in PGPtray initialisieren und beenden 186
Sicherheitsverbindung. Siehe “SA”
Sicherheitsverknüpfung (Security Association, SA)
initialisieren 181
ungültig werden 180
Sichern einer Netzwerkkarte 199
Sitzungsschlüssel
Definition 314
Smurf, Angriff 295
Speichern
aktive SAs 190
Protokollinformationen 198
Schlüssel 51
SSL (SSL-Protokoll, Secure Socket Layer)
Definition 314
Standardeinstellungen
für PGPnet 276
Standardschlüsselpaar
festlegen 73
Standby-Modus
PGPdisk-Volumes entladen 281
Starten
PGPnet 183, 222
PGPtray 36
Status (Registerkarte) 187
Eigenschaften 190
Statusleiste 188
Suchen auf dem Schlüsselserver 59
Symmetrischer Algorithmus
Definition 314
SYN Flood, Angriff 295
Systemfeld in der Task-Leiste
PGP verwenden 36

T

Tasks
geplantes Bereinigen von freiem Speicherplatz 136
Tastaturbefehl
festlegen 281
Teardrop, Angriff 295
Technischer Kundendienst
notwendige Informationen 21
online 21
Teilen von Schlüsseln oder “Geheimnisverteilung”
Definition 314
Teilen, Schlüssel 55
Teilnetze
ändern 233
entfernen 233
Teilschlüssel
Definition 314
Eigenschaften 85
entfernen 85
Größe 85
Gültigkeit 85
neu erstellen 85
zurücknehmen 85
TEMPEST-Angriffe

siehe auch “Sichere Darstellung”
Text
Definition 314
Textausgabe 130
TLS (Transport Layer Security)
Definition 314
TLSP (Transport Layer Security Protocol)
Definition 314
Transportmodus
Definition 180
Triple-DES-Algorithmus 260
Definition 314
Tunnelmodus
Definition 180
Twofish-Algorithmus 260
Definition 315

U

Überblick
Schlüsselkonzepte 41
Übernahme einer TCP-Sitzung
Definition 315
Überprüfen
Echtheit von Schlüsseln 62
Fingerabdrücke 91
Schlüssel
autorisierte Schlüsselverwalter 65
höhergestellter Schlüsselverwalter 65
öffentliche Schlüssel 31, 64
Vertrauen aussprechen 80
UDP Flood, Angriff 295
Ungültig werden
SAs 180
Ungültige Nutzinformationen 287
Ungültiger Austausch 287
Ungültiges Cookie 288
Unsicherer Host
Definition 180
Unsicheres Teilnetz
Definition 180
Unterschreiben 73
Definition 315
E-Mail 32, 111, 123
mit geteilten Schlüsseln 132
öffentliche Schlüssel 64, 78
Schlüssel 78
autorisierter Schlüsselverwalter, Beschreibung 65
höhergestellter Schlüsselverwalter, Beschreibung 65
Unterschrift
Definition 315
Unwiederherst. löschen
Dateien 132
Urheberrechtsnachweis
Definition 315

V

Verfälschen
eigene Schlüssel schützen 51
Vergessene Paßphrase 52
Vergleichen
Schlüsselfingerabdrücke 63
Verifizieren
Echtheit von Schlüsseln 62
E-Mail 124, 126
Verifizierung
Definition 315
Verknüpfungen, HotKeys 253
Verschlüsseln

E-Mail 32, 111, 123, 124, 126
für Gruppen 121
für Sie selbst 245
ICQ-Nachrichten 141
Kopie mit eigenem Schlüssel 245
über die Zwischenablage 36
Verschlüsselung
Definition 315
Verschlüsselungsoptionen
Algorithmen 260
Dateien
konventionell 131
Original endgültig löschen 130
selbstentschlüsselnde Datei 131
Sichere Darstellung 130
Textausgabe 130
E-Mail
konventionelle 116, 119
Sichere Darstellung 116
festlegen 245
Verschlüsselungssystem
Definition 315
Verteilen
öffentliche Schlüssel 55
Verteilerlisten
Gruppen erstellen 122
Gruppen löschen 122
Gruppen verknüpfen 123
Gruppenlisten Elemente hinzufügen 122
Mitglieder löschen 122
Vertrauen
für Schlüsselüberprüfungen aussprechen 80
Vertrauenswürdig
Definition 315
Verwalten
Schlüssel 67, 244
Verwenden
PGP
über das Systemfeld 36
über die Zwischenablage 36
Virtual Private Networks (VPNs)
Siehe auch “VPN” und “Virtuelle Private Netzwerke (VPNs)”
Virtuelle Identität
aktivieren 232
Definition 315
Virtuelle Private Netzwerke (VPNs)
Definition 175
Vollmacht
Definition 316
Vollmachtszertifikat
Definition 316
Volumes
entladen 159
laden 158
Volumes entladen
automatisch 281
Vordefinierte Firewall-Schutzgrade 203
Überblick 201
Voreinstellungen
festlegen 36
Vorschläge
Definition 309
festlegen 273
VPN (Virtual Private Network)
Authentisierungsoptionen
entfernte Authentisierung 269
Verbindungen authentisieren 268
Beschreibung 178

Definition 316

Dynamisches VPN 264

erweiterte Optionen

Höchste Geheimhaltung beim Weiterleiten 275

Vorschläge, 273

zulässige entfernte Vorschläge 271

VPN (Registerkarte in PGPnet) 187

W

Web of Trust

Definition 316

Weitergeben

eigene öffentliche Schlüssel 55

öffentliche Schlüssel 31

PGPdisk-Volumes 164

Wiederherstellen

Standardeinstellungen für PGPnet 276

Windows-Explorer

PGP verwenden 35

Wörterbuch-Angriff

Definition 316

X

X.509-Zertifikate 258

abrufen 95

Definition 316

einem Schlüsselpaar hinzufügen 81

für Verbindungsauthentisierung verwenden 267

hinzufügen

Root-CA-Zertifikate 92

importieren 62

zum Schlüsselbund hinzufügen 96

Z

Zeilenumbruch 252

Zeitangaben

Definition 316

Zertifikat (digitales Zertifikat)

Definition 316

Zertifikate

X.509-Root-CA-Zertifikaten zum Schlüsselbund hinzufügen 96

Zertifizieren

Definition 316

öffentliche Schlüssel 31

Zertifizierung

Definition 316

Zertifizierungsinstanz

Definition 316

Optionen festlegen 258

Zufallszahl

Definition 317

Zugeordneter Rücknahmeschlüssel

Eigenschaften 87

Zulässige Algorithmen 261

Zurücknahme

Definition 317

Zurücknehmen

Schlüssel 90

Zusammensetzen von geteilten Schlüsseln 99, 100

Zwischenablage

PGP verwenden 36